UPDATED LEGACY APPLICATION TRANSITION GUIDE

22 August 2003

SUBMITTED BY

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
10260 CAMPUS POINT DRIVE, LOC 973, M/S T-1
SAN DIEGO, CALIFORNIA 92121

PREPARED FOR

COMMANDER
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127

UNDER CONTRACT WITH

FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT CENTER
FALLS CHURCH, VA 22041

CONTRACT NUMBER: GS00K96AJD0014
TASK ORDER: T0002AJM032
TDL NUMBER: 1504
CDRL NUMBER: D005
TITLE: UPDATED LEGACY APPLICATION TRANSITION GUIDE

Legacy Applications Transition Guide (LATG) v5.1

(Rapid Certification Phase)

August 22, 2003

Prepared by:

NMCI Program Management Office – Technical Execution Division, PMW 164-4
Space and Naval Warfare Systems Command
Participants in the creation of this guide include:
Department of the Navy, Chief Information Officer
Program Executive Office – Information Technology
Electronic Data Systems
Customer Representatives from the Application Enterprise Action Group

Prepared for:

All NMCI Customers

Record of Document Changes

Change No. & Date of Change	Date of Entry	Page Count Verified by (Signature)
1.0	14 March 2001	
1.1	18 April 2001	
2.0	13 July 2001	
2.1	26 October 2001	
3.0	19 April 2002	
4.0	30 June 2002	
4.1	15 August 2002	
5.0	15 February 2003	
5.1	22 August 2003	

For questions or suggestions to improve this guide please contact:

Space and Naval Warfare Systems Command (SPAWAR) Navy Marine Corps Intranet (NMCI) Program Management Office (PMO) San Diego, California

PMW 164-4, Technical Execution Division, Legacy Applications
619-524-7435

Electronic Data Systems
619-817-3856

AMENDED SECTIONS FOR THIS RELEASE
(HIGHLY Recommend Reviewing These Sections)

These are amended sections of this version of the Legacy Application Transition Guide. It is highly recommended that the reader, at the bare minimum, read the updates listed herein.

General updates to sections of this guide are listed as Updates, Additions, and Deletions. Updates and Addition refer to sections located in this guide, whereas Deletions pertain to the last LATG version (in this case v5.0, dated 15Feb03).

UPDATES

- General Document Updates
  - Replaced any reference from ISF to EDS
- Section 1.0
  - Developed New Introduction
  - Amended verbiage
  - Provided more detailed information
- Section 2.0 – No changes to report
- Section 3.0
  - Amended verbiage
  - Section 3.2 – Navy Information Office
  - Section 3.2.1 – Navy Applications Database Task Force
    - Amended verbiage
  - Section 3.2.2 – Functional Area Manager
    - Amended verbiage
    - Updated bulleted information
  - Section 3.2.4 – NMCI Designated Approval Authority
    - Updated verbiage
  - Section 3.3.1.6.1.3 – Site Transition Execution Manager
  - Section 3.3.1.6.1.4 – Information Assurance Tiger Team
  - Section 3.3.1.6.2.1 – Site Delivery Manager
  - Section 3.3.1.6.2.2 – Site Transition Manager
  - Section 3.3.1.6.2.3 – Project Coordinator
  - Section 3.3.1.6.3 – Electronic Data Systems
- Section 4.0
  - Fig. 4-1 – Updated
  - Fig. 4-3 – Updated
  - Fig. 4-5 – Updated
  - Section 4.1.3 – Establish Contact with PMO and EDS
    - Updated verbiage
  - Section 4.1.10 – DON application and Database Management System (DADMS)
    - Updated verbiage
  - Section 4.2.3.2 – Create User List and Begin Application Mapping
  - Section 4.2.3.3 – Creating a Rationalized List in ISF Tools
    - Updated verbiage
  - Section 4.2.4 – Create User List and Begin Application Mapping
    - Updated verbiage
  - Section 4.2.6 – Creating a Request for Service in ISF Tools
    - Updated verbiage

- Section 4.2.7 Linking Application to Implementation Groups in ISF Tools
  - Updated verbiage
- Section 4.2.8 Gather In-Use Peripherals and Drivers
  - Updated verbiage
- Section 4.2.12 Implementation Groups (IG)
  - Updated verbiage
- Section 4.3.4.3 – Apply NMCI Rulesets
  - Updated verbiage
- Section 4.4. – COLLECTION
  - Updated Verbiage
- Section 4.4.1.2 - Command RFS and Rationalized List
  - Updated verbiage
- Fig. 4-6 – Updated
- Section 4.4.4 – Perform Final Application Mapping
  - Updated verbiage
- Section 4.5.1 – Initial Assessment and Testing Decision
  - Updated verbiage
- Section 4.6.2 – San Diego Packaging & Certification
  - Updated verbiage
- Section 4.6.3 – Pop-In-A-NOC (PIAN)
  - Renamed Complex Application Lab
  - Updated verbiage
- Fig. 4-10 – Updated
- Section 4.6.5.1 – PIAB Package and Push
  - Updated verbiage
- Fig. 4-11 – Updated
- Fig. 4-12 – Updated
- Section 4.7.2 – Information Assurance
  - Updated verbiage
- Section 4.7.4 – Risk Mitigation
  - Updated verbiage
- Fig. 4-13 – Updated
- Fig. 4-14 – Updated
- Section 4.8.1 Legacy Application Deployment Readiness Activity
  - Updated verbiage
- Section 4.8.2.2 – Quarantine Remediation
  - Updated verbiage

- Section 5.0 – No changes to report
- Appendices
  - Appendix A – Legacy Applications POA&M Template
    - Updated verbiage
  - Appendix B – Gold Disk Standards
    - Updated verbiage
  - Appendix C – Late Application Identification and Submission Process
    - Updated verbiage
  - Appendix E – NMCI Application Ruleset
    - Updated to v 2.96
  - Appendix F – Classified Legacy Applications Transition Process
    - Updated verbiage
    - Fig. F-2 – Updated
    - Fig. F-3 – Updated

        - Fig. F-4 – Updated
        - Fig. F-5 – Updated
        - Fig. F-6 – Updated
        - Fig. F-7 – Updated
        - Appendix F 3.5.3 – Classified Complex Application Lab
            - Update for Pop-In-A-NOC
        - Appendix Fig. F-10, Pop-In-A-NOC
            - Updated
        - Appendix Fig. F-11, Classified Pop-In-A-BOX
            - Updated
        - Appendix Fig. F-12, Classified LDSD&T
            - Updated
        - Appendix Fig. F-13, Classified Pre-Deployment
            - Updated
    - Appendix G, Templates, Samples, and Examples
        - Updated Sample Forms
    - Appendix I – Glossary
        - Updated Definitions
    - Appendix J – Acronym List
        - Updated Acronyms

ADDITIONS

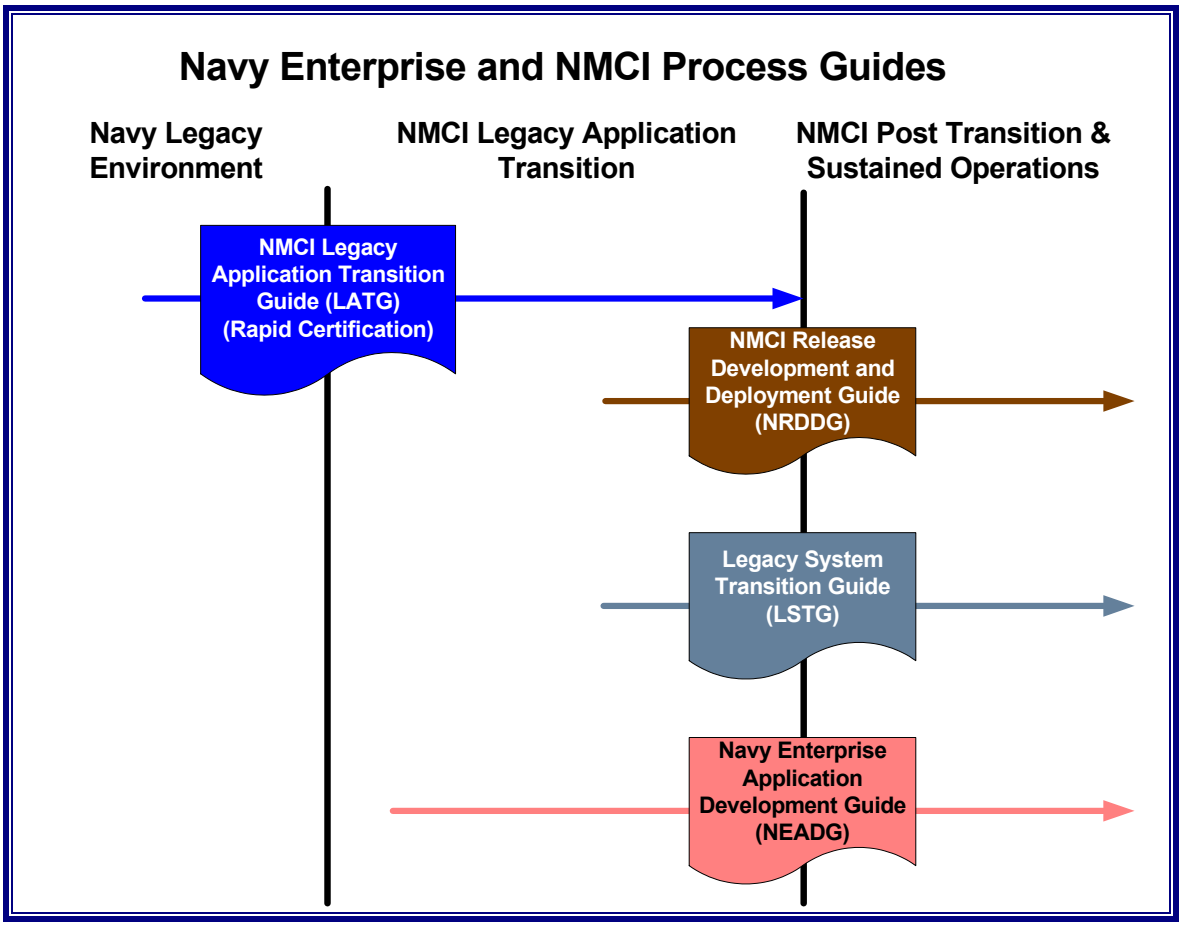
- Section 1.0
    - BACKGROUND - page 1-1
    - PURPOSE - page 1-1
    - OBJECTIVES - page 1-2
    - SCOPE - page1-2
- Section 2.0 – No changes to report
- Section 3.0
    - Section 3.2.1 – NADTF related bullets
    -
    - Section 3.3.1 – Site Management Division, PMO
    - Section 3.3.1.1 – Regional Classified Implementation Team
    - Section 3.3.1.2 – Regional Organization
    - Section 3.3.1.3 – Transition Organization
    - Figure 3-1 – JECC ORG Chart
    - Section 3.3.1.4 – Enterprise Roles and Responsibilities
    - Section 3.3.1.4.1 – Government Enterprise
    - Section 3.3.1.4.2 – EDS Enterprise
    - Section 3.3.1.5 – Regional Roles and Responsibilities
    - Section 3.3.1.5.1 – Government Regional Integration Lead
    - Section 3.3.1.5.2 – EDS Regional Transition Manager & Regional Delivery Manager
    - Section 3.3.1.6 – Site Roles and Responsibilities
    - Section 3.3.1.6.1 – Government
    - Section 3.3.1.6.1.2 – Customer Technical Advisor
    - Section 3.3.1.6.2.1 – Site Delivery Manager
    - Section 3.3.1.6.2.2 – Site Transition Manager
    - Section 3.3.1.6.2.3 – Project Coordinator
    - Section 3.3.3.2.1 – Quick Look Assessment Team

- Section 3.4.2 – Customer Project Manager
- Section 4.0
  - Section 4.2.3 – Concurrent Process
  - Section 4.2.4.1 – NMCI – Enterprise Tools (NET)
  - Section 4.2.8.4 – Peripheral Transition
  - Fig. 4-4 – Example of Delivery Process
  - Section 4.3.4.3.1 – FAM Waiver Process
  - Section 4.3.4.7 Adding an Application to the Legacy Applications Rationalized List
  - Section 4.3.6 – Compare Application Usage to Application List
- Section 5.0 – No changes to report
- Appendices
  - Appendix D – Pertinent Naval Messages
    - Added messages
  - Appendix F – Classified Legacy Applications Transitions Process
    - Added Classified Rationalized List Template

DELETIONS From LATG (v5.0, 15Feb03)

- Section 1.0 – No deletions to report
- Section 2.0 – No deletions to report
- Section 3.0
  - Section 3.2.1 – Page 3-6
    - Deleted bullets pertaining to FAM, GOTS, and COTS
  - Section 3.3.1 – Customer Project Manager
  - Section 3.3.3.1 – Legacy Application Site Visit Team
  - Section 3.5.1 – Site Manager
  - Section 3.5.2 – Product Delivery Manager
- Section 4.0
  - Section 4.2.3 – Concurrent Process
  - Section 4.2.3.2.1 – NMCI Ordering Interface System
    - Replaced by Section 4.2.4.1 NMCI Enterprise Tools (This Guide)
  - Section 4.3.4.3.1 – Killed Applications
  - Section 4.3.4.3.2 – Failed Applications
  - Section 4.3.5 – Apply UTAM
  - Fig. 4-24 – NMCI Quarantined Desktop Application Remediation
  - Section 4.8.2.3 – Prioritization
  - Section 4.8.2.4 – Administrative Failure Analysis
  - Section 4.8.2.5 – Technical Failures
  - Section 4.8.2.5.1 – Deployment Failure Transition Strategy
- Section 5.0 – No deletions to report
- Appendix F
  - Section 3.6 – Classified Application Transition Documentation

NMCI PROCESS GUIDES



THIS FIGURE ILLUSTRATES HOW THE VARIOUS NMCI PROCESS GUIDES COME INTO PLAY THROUGHOUT THE LIFECYCLE OF THE NMCI PROGRAM

LEGACY APPLICATIONS TRANSITION GUIDE (LATG)

The Legacy Applications Transition Guide (LATG) presents a complete baseline overview of the Legacy Applications Rapid Certification Phase of the Legacy Applications Transition Process. It is for Navy Marine Corps Intranet (NMCI) customers involved with transition activities. Electronic Data Systems (EDS) and Government program management personnel worked in close cooperation to design the processes, procedures, and policies described in the LATG. The Guide describes in detail the roles and responsibilities of those organizations and positions involved in transitioning Legacy Applications through the Rapid Certification Phase.

LEGACY SYSTEMS TRANSITION GUIDE (LSTG)

The Legacy Systems Transition Guide (LSTG) provides both an approach and the associated processes to successfully transition systems from legacy environments to the NMCI environment while maintaining or improving system performance and availability. The LSTG provides the Site Representative, Central Design Authority (CDA), and the Program of Record/Program Manager

(POR/PM) with the unique processes, tools/templates, and documentation guidelines to plan and execute the transition of their respective systems to the NMCI environment.

NMCI RELEASE DEVELOPMENT AND DEPLOYMENT GUIDE (NRDDG)

The NMCI Release Development and Deployment Guide (NRDDG) is a consolidated source of information, guidance and direction for developers and application owners who build and/or modify applications as well as for the acquirers of applications intended for use within NMCI. As a supplement to the Navy Enterprise Application Development Guide (NEADG), the NRDDG is written to support the Central Design Authority (CDA) in the development and deployment of releases that will operate within NMCI. For web based application guidance, the user should refer to the NEADG, the TFW and NEP. NRDDG fulfills an intermediary requirement in bridging the gap between present application development cycles underway by the CDAs and the target state of web-enablement of all Navy Enterprise applications under the Task Force Web initiative.

NAVY ENTERPRISE APPLICATION DEVELOPMENT GUIDANCE (NEADG)

The purpose of the Navy Enterprise Application Development Guidance (NEADG) is to provide detailed information and direction to developers tasked with migrating applications, content, and services into the DON Enterprise IT Environment. This effort seeks to align current software development community practices within the Navy and Marine Corps with the best practice vision embraced by the DON and DOD. Their vision is of web enabled enterprise applications that are extensible, scalable, and open in their use of current standards and leading edge technologies. Additionally, the NEADG seeks to present guidance information in a way that is easily human and machine searchable and that adds value for the information consumer by aligning the guidance to their specific activities and roles. This will be accomplished by mapping constituent guide content to searchable metadata categories that will allow distinct renderings or views of the original data. The web-based platform will enable the collection and packaging of content from other guides focused on the overall purpose of guiding CDAs in transitioning applications toward the DON Enterprise IT Environment.

TABLE OF CONTENTS

APPENDICES

TABLE OF FIGURES

1.0 INTRODUCTION

This document presents a baseline overview of the Legacy Applications Rapid Certification Phase of the Legacy Applications Transition Process. It has been developed for Navy Marine Corps Intranet (NMCI) customers involved with transition activities. Electronic Data Systems (EDS) and Government program management personnel worked in close cooperation to design the processes, procedures, and policies described herein. This document exists to provide clarification of the actions and responsibilities associated with the process of transitioning Legacy Applications into the NMCI enclave.

1.1 BACKGROUND

The Naval message of 25 Feb 02 released by CNO N09T (date-time-group 252250Z FEB02) mandated Certification Phase transition guidance for NMCI. Director NMCI released a coordinated Naval message COMSPAWARSYSCOM/PMW164 242225Z MAY 02 with the Navy and Marine Corps Program Offices and EDS. This message further refined the transition processes in order to improve and accelerate near-term NMCI seat rollout. The new process, which titled the "Rapid Certification Phase", reflects the process and procedural changes outlined in these pertinent messages. These messages focused on three keys to success as customers begin work on NMCI transition:

1. Site and Echelon II use of the ISF Tools Database (described here).
2. Reduction in the number of applications (guidance provided here).
3. Removal of certain accreditation requirements prior to seat Cutover to the Risk Mitigation Phase (guidance described elsewhere).

COMNAVNETWARCOM Message DTG R 021936Z MAY 03 discusses responsibilities and actions in association with the 2003 NMCI "Rapid AOR" initiative. The NMCI program will be pursuing an aggressive initiative termed "Rapid AOR" for expediting NMCI seat rollout. NETWARCOM messages outline AOR-related NMCI requirements and assign specific responsibilities to the site representatives, EDS, NMCI Directors, and Program Management Office (PMO).

1.2 PURPOSE

The end result of accomplishing activities associated with the NETWARCOM messages is a positive step towards achieving centralized Information Assurance (IA) management in a new network-centric Navy communication infrastructure. These activities set the stage for transitioning "stovepipe" legacy networked applications into an enterprise-wide computing environment with industry standard architecture and services, and uniformly higher levels of security.

PMO has published this LATG based on field experience, and considers the exhibited level of effort (LOE) sufficient to meet the requirements of NETWARCOM. This is a guidance document that offers "best practice" advice with the recognition that site-specific tailoring will be required. The LOE experience of larger sites will not equal that of smaller sites due to the obvious complexities typically associated with larger infrastructures.

1.3 OBJECTIVES

This document provides the guidance, will create a consistent method of data gathering, packaging, and submission. Consistency is critical to expediting the execution of required actions and will help avoid expenditures of resources in areas currently not in the scope of the assigned actions.

The Chief of Naval Operations (CNO) has assigned specific responsibilities to Echelon II Commanders for identification, rationalization, submission, and accreditation of applications. The NMCI Legacy Applications Transition is divided into two distinct phases:

1. Rapid Certification Phase (covered in this guide)
2. Risk Mitigation Phase (covered in the Legacy Server Transition Guide (LSTG))

1.4 SCOPE

The scope of this guide is limited to the processes, procedures, and guidelines associated with transitioning systems from legacy Department of the Navy (DON) or Department of Defense (DoD) environments into the NMCI environment. The LATG presents a complete baseline of the Rapid Certification Phase of the Legacy Application Transition Process. This Guide describes in detail the roles and responsibilities of those organizations and positions involved in transitioning Legacy Applications in addition to a detailed discussion of the Rapid Certification Phase. A Legacy Application is an application that is currently in use by an individual performing missions or business for the DON. Legacy Applications are not elements of the standard set service, which is also known as the "Gold Disk".

This guide is focused on the processes, procedures, and guidelines for transitioning DON and DoD legacy applications into the NMCI environment. This Guide describes in detail the roles and responsibilities of those organizations and positions involved in transitioning Legacy Applications.

What is a Legacy Application?

A Legacy Application is an application that is currently in use by an individual performing missions or business for the DON. Legacy Applications are not elements of the standard set of services, which is also known as the "Gold Disk".

The NMCI contract states, "An existing customer software application that is not included in the NMCI standard seat services or the CLIN 0023 catalog."

Why Transition Legacy Applications to NMCI?

We are transitioning applications to NMCI because NMCI is the new information technology (IT) environment for the Navy and Marine Corps. Secondly, Legacy Application transition will enhance security, improve standardization, reduce duplication/redundancy, and minimize software support costs. With this paradigm shift, customers should make every effort to eliminate obsolete, redundant, and nonstandard applications. They should do this in concert with their Echelon II Commanders.

Classified Legacy Application Transition Process

The Classified Transition processes are similar to the unclassified process, with the following exceptions:

- Special handling procedures
- Separate Application Integration and Testing (AIT) Lab
- Special Request for Service (RFS)
- Manual Tracking System (excludes the use of the ISF Tools Database)

The Classified Legacy Applications Transition Process and its differences are discussed in Appendix F of this guide.

Let us begin with the Legacy Application Transition Process.

2.0 OVERVIEW OF LEGACY APPLICATIONS TRANSITION PROCESS

An overview of the NMCI Legacy Applications Transition Process is provided in Figure 2-1. Note the clear distinction between the Rapid Certification Phase and the Risk Mitigation Phase. The Legacy Applications Transition of any site follows the pattern from left to right.

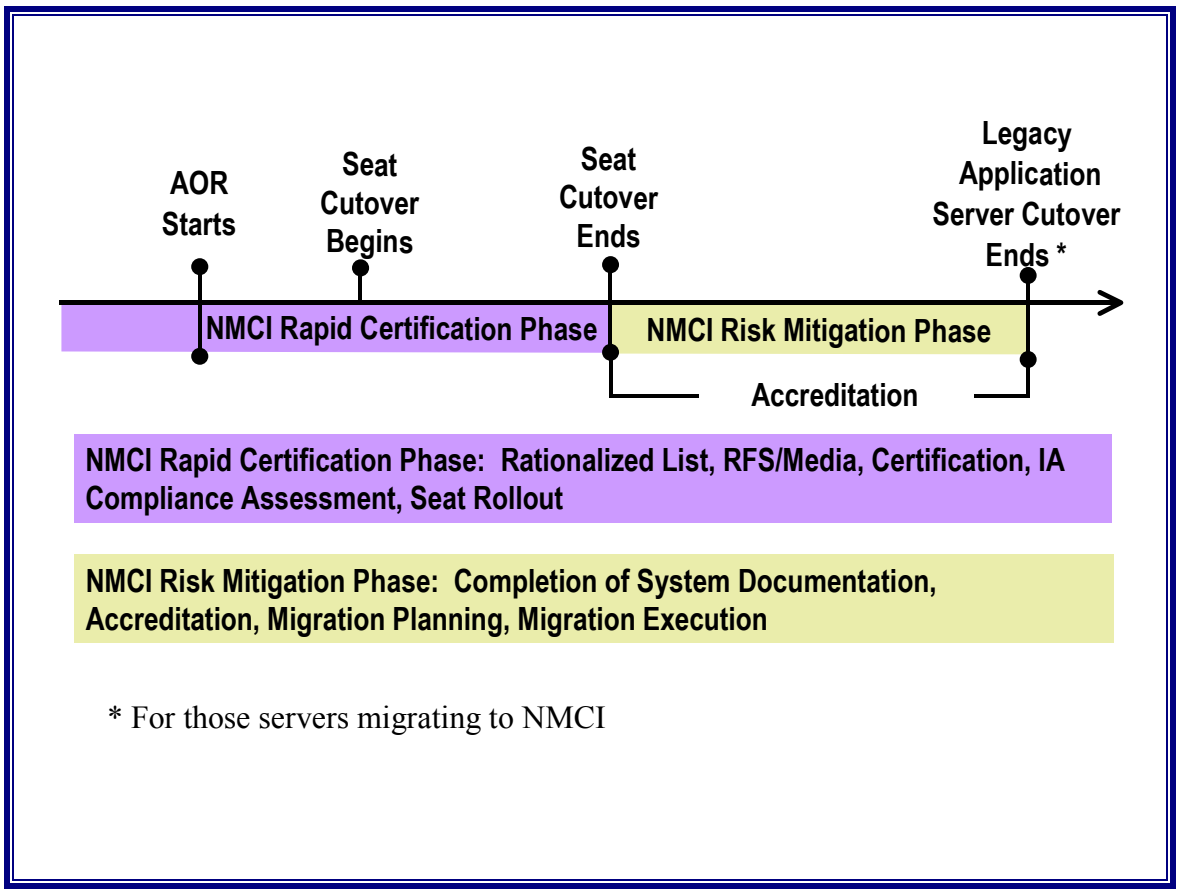


Figure 2-1. Overview of NMCI Legacy Applications Transition Process

The Rapid Certification Phase (purple) includes AOR, Seat Cutover (begin) and Seat Cutover (end). The Risk Mitigation Phase (tan) begins when Seat Cutover has completed and continues until the completion of server migration.

Note the purple and tan bars below the timeline in Figure 2-1. These different views show the critical activities and milestones associated with each phase. These contain the main portion of information crucial to transition success. All of these are explained in greater detail in Section 4.0 of this guide. Within the Rapid Certification Phase, customers will become involved with:

- The creation of a Rationalized List of applications
- The submission of RFSs and application media to EDS
- Functional testing of the application
- Completion of the IA compliance assessment by the EDS

Within the Risk Mitigation Phase, information regarding system documentation, transition planning, and accreditation will be required. The Risk Mitigation Phase is *not* the focus of this document.

Figure 2-2 depicts the end-to-end transition process showing the major Command and Contractor Deliverables. It breaks down the Rapid Certification Phase into smaller processes describing the 'life of a transitioning application.' Each of these sub- processes will be further discussed in Section 4.0 of this guide.

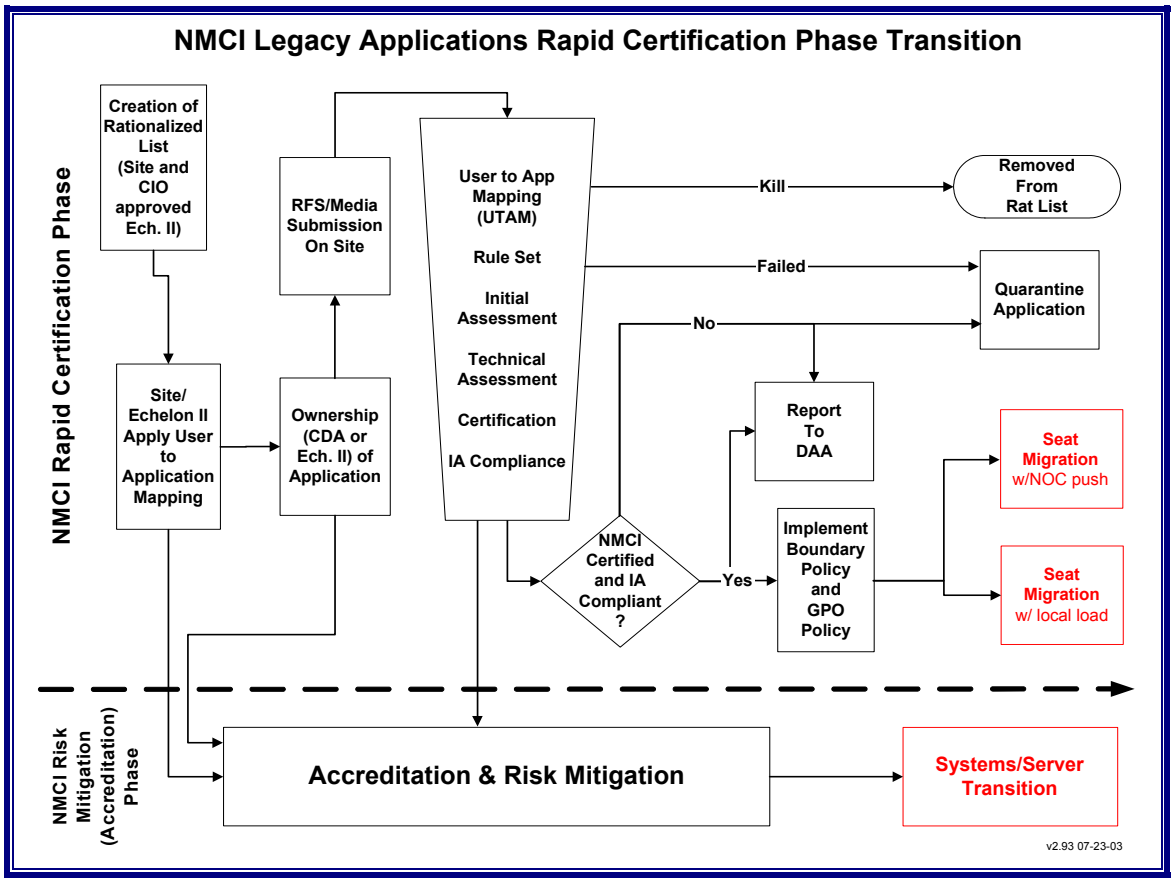


Figure 2-2. NMCI Legacy Application Transition

3.0 ROLES AND RESPONSIBILITIES

The Legacy Systems Transition Process is accomplished using resources of the Navy Information Officer (IO), Functional Area Managers (FAM), Program Management Office (PMO), EDS, Echelon II, Central Design Authority (CDA) and the Command/Site. This section describes the roles and responsibilities of the Legacy Applications Transition Program.

3.1 DIRECTOR NMCI

Director NMCI is managing the acquisition of NMCI. The incumbent reports to the Assistant Secretary of the Navy for Research Development and Acquisition (ASN RDA); functions within the policy constraints of Department of Defense (DoD) acquisition regulations; and provides additional acquisition guidance to the Navy and Marine Corps NMCI Program Managers (PMs).

3.2 NAVY INFORMATION OFFICER (IO)

The Navy IO is responsible for bringing operational Information Technology/Information Management (IT/IM) requirements into alignment with Navy functional capabilities using established processes and procedures. The Navy IO advises and assists the CNO in achieving network-centric operational capabilities by managing robust global and local networks. The Navy IO employs proven-successful business practices integrates IT/IM applied to warfighters at sea, and the supports shore establishment. Additionally, the Navy IO oversees the integration of dispersed sea-based and Joint Command Control architectures in supply chain and enterprise resource management, the Navy IO champions the incorporation of industry's significant improvements in IT into the Navy enterprise.

The Navy IO leads the development of strategic plans and implementation policies for managing global Navy enterprise IT solutions across the Navy. The Navy IO receives requirements from, and provides policies and procedures to, the Commander, Naval Network Warfare Command (NETWARCOM) who is responsible for its implementation. NETWARCOM assumes the duties of Designated Approving Authority (DAA) for all operating, general service, Navy IT systems and networks. This guidance is referenced in Appendix D22.

The Navy IO current focus is on the reduction of Navy legacy applications, supporting rapid transition to NMCI; supporting the establishment of FAMs that will be responsible for all software applications and databases within their functional area; developing the process for procuring enterprise software licenses for applications that are in use Navy-wide; and leveraging the capabilities of the NMCI to enhance operations and communications within the Navy. In addition, the Navy IO shall be responsible for the following:

- Ensure that IT/IM requirements are consistent and compliant with overall Navy/DoD architectures and investment decisions. The Navy IO will work closely with the DON and the U.S. Marine Corps Chief Information Officers (CIO) to manage "Information" and "Knowledge" as key strategic resources in order to satisfy Fleet information requirements.
- Oversee the development and implementation of systems, policies and processes to ensure integrity, availability and authentication and the safeguarding of Navy information, and display, processing and storage systems. Substantiate Navy compliance with evolving national security

Information Assurance (IA) policies through the acquisition and implementation of approved IT/IM products.

- Establish, manage, and enforce IT/IM configuration standards for hardware, software, and network connectivity. Oversee the development of an enterprise management process for IT/IM configuration control.
- Lead the Navy effort in support of the DoD and DON CIO's efforts to develop, maintain, implement, and evolve DoD Joint information architectures. Serve as the Navy's lead Point of Contact (POC) for interaction and coordination with other Service, Joint, DoD, and interagency CIOs for implementing the Global Information Grid enterprise solutions.
- Develop, coordinate, and ensure compliance with the Navy's IT/IM Plan, which serves as a key input to the IT/IM Strategic Plan. The term "information technology" includes "national security systems" as defined in the Clinger-Cohen Act of 1996.
- Advise the CNO and other senior leadership on all IT/IM-related issues. Key to this function is close coordination and frequent liaison with U.S. Marine Corps CIOs, the Fleet Commanders, Systems Commands, NETWARCOM, and Major Claimant CIOs.
- Support DoD and CIOs' efforts to promote effective and efficient design and operation of information management processes throughout the global Navy enterprise.
- Review and critique all Navy IT/IM Support Plans (C4I Support Plans), prepared and updated at each acquisition milestone in accordance with DoD 5000-series directives, to verify compliance with DoD Joint Technical Architectures and to ensure interoperability, compatibility and integration with other Joint warfighting and support systems.
- Oversee implementation of a Navy-wide IT/IM systems-of-systems testing program to ensure continued interoperability.
- Develop and implement knowledge management strategies that facilitate the improved creation and sharing of knowledge. Knowledge management, which involves delivering the right information to the right decision-maker at the right time to create the right conditions for new knowledge, enables more effective and agile decision-making, resulting in greatly improved mission performance.
- Promote results-based performance measures and best practices to improve mission performance and optimize the return on investment for IT/IM.

3.2.1 Navy Applications Database Task Force (NADTF)

The NADTF was established in March 2002 to act as the focal point for the Navy in developing a reliable inventory of legacy software applications. The NADTF is responsible for:

- Reviewing and comparing DADMS and ISF Tools Database for NMCI applications to maintain consistency between the two databases.
- Assisting the FAMs in the execution of their process by providing coordination between the FAMs, Echelon II Commands, CDAs, DAAs, and NMCI Program Management Office (PMO).
- Application, development, and refinement of the NMCI NADTF rule set in DADMS and ISF Tools Database.
- Assisting in the standardization of Government Off the Shelf (GOTS) and Commercial Off the Shelf (COTS) applications and databases on Navy Networks.

- Coordination of action with Echelon II Commands and NETWARCOM for removal of applications from NMCI based on FAM decisions.
- Overseeing Navy-wide legacy application identification.
- Coordinating (through Program Management Office (PMO) San Diego) the entry of needed application information changes into the ISF Tools Database.
- Identifying the Program of Record (POR)/CDAs for legacy applications.
- Identifying a standard version for the Government Off the Shelf (GOTS) applications.
- Working with the PEO-IT Enterprise Solutions Office and Department of the Navy Chief Information Officer (DON CIO) to identify recommended Commercial Off the Shelf (COTS) application products and product versions so the Navy can acquire required Enterprise Licenses.
- Working with other Navy groups, such as the NMCI Program Office, PEO-IT's Enterprise Solution Office (ESO) and TFW to maintain synergy and prevent duplication of efforts. The NADTF reports directly to the Navy IO (OPNAV N-6/7) and the Director, NMCI to reduce the number of applications that must be integrated into NMCI through:
    - Elimination of inappropriate applications.
    - Standardization of application versions.
    - Recommending applications be quarantined if the application violates established security parameters.
    - Recommending applications be rejected if media is not available at an appropriate time prior to cutover.
    - Providing other recommendations that will enhance the ability to roll NMCI seats while weighing the costs versus benefits to the individual commands.

NADTF was established to provide a comprehensive approach for identifying and reducing the number of software applications being used by the Navy. This process was undertaken in cooperation with the NMCI PMO in San Diego. The process consisted of reviewing the initial application data call that had been entered into the EDS application database. NADTF standardized the naming convention to eliminate duplicate entries, and eliminated applications and its components that could not operate within the - NMCI Windows 2000 environment. Specifically, the Task Force's objectives were to:

- Scrub Implementation Groups Rationalized Lists to identify issues to resolve prior to NMCI implementation.
- Identify all Navy software applications, whether or not they would be required to run in the NMCI environment.
- Facilitate entry of software application information data into the ISF Tools Database.
- Take the lead in standardizing software application terminology (name, version, etc.), including serving as the final authority for establishing the naming convention for all software applications (including version designation).
- Provide recommendations to standardize to a limited number of software versions, which would reduce the number of software applications required to be implemented into the NMCI environment.

- Enhance Navy awareness and knowledge of the NMCI implementation process.
- Provide regular status reports on progress achieved in reducing the number of legacy applications to the OPNAV and Secretary of the Navy staffs.

As commands commenced the cutover to NMCI the role of the NADTF changed in response to specific problems that were being encountered during seat rollout. Some of the major initiatives that are underway include:

- Identifying the CDA for each GOTS application.
- Identifying those software applications that are not on the Gold Disk but are widely used throughout the Navy. The intent is to identify ways the Navy could acquire enterprise licenses to reduce the cost of ownership of these applications for each command and across the enterprise.
- Recommending GOTS and COTS applications (by version) that should be established as standard applications within the Navy.
- Refining the NMCI Legacy Application Ruleset for applications. This Ruleset determines the criteria that must be met for an application to be permitted to operate within NMCI.
- Working closely with the NMCI Designated Approval Authority (DAA) ensuring the NMCI security posture is not compromised by non-compliant applications.

As the rollout of NMCI accelerates and the number of NMCI users increases, it is expected that the role of the NADTF will continue to change in response to user demands. As more experience is gained with the NMCI network, policies and procedures will be established to standardize operating procedures across the Navy. The NADTF can begin to address the integration of NMCI with other command and control networks within the Navy.

3.2.2 Functional Area Manager (FAM)

By June 2003, there were more than 34,000 legacy applications identified for transition to NMCI. This number of applications represents a huge investment in licensing, maintenance and operating expenses; therefore, the Under Secretary of the Navy designated the FAMs to implement processes reducing the number of IT applications by 95%, to the minimum number required to support Naval requirements. This reduction process will involve standardizing to single application versions, selecting certain applications or suites of applications to perform specific Navy-wide functions, Reduction will also entail eliminating applications that will not operate within the NMCI environment. FAMs are responsible for the enterprise management of applications and databases assigned within their functional areas. Therefore, ***only applications that have been accepted and approved by the FAMs will be deployed in NMCI***.

FAMs are appointed by OPNAV, and are responsible for overall enterprise software management and the execution of specific responsibilities that include, but are not limited to, the following:

- The FAM identifies and appoints the Functional Lead and Technical Lead for process execution. On behalf of the FAM, the designated Functional Lead (FAM Lead) communicates formal intent and/or commitment to fully support FAM Mid-Term Application and Database Rationalization Process execution. The Functional Lead provides management oversight for process scheduling, resources, execution, and integration.

  - The Technical Lead may be a contractor or in-service government individual. At the discretion of the FAM, a contractor may be procured to form the basic FAM Team/FAM Partnership Team and to execute this entire process with assistance from designated Functional Area (FA) Subject Matter Experts (SMEs). FA SMEs may be tasked to support contractor efforts on a full, or part time basis.

- To execute the FAM Mid-Term Application and Database Rationalization Process, it is recommended that the FAM Short-Term Application and Database Rationalization Process personnel be used.
- The designated Functional Lead identifies and appoints the FAM Team/FAM Partnership Team, with FAM approval. The FAM Team/FAM Partnership Team provides the necessary expertise to execute the full spectrum of FA business and operational requirements analysis and validation for the functional areas designated by Navy Leadership.
- The FAM is responsible for overseeing the activities of Functional Data Managers (FDMs).
- The key to successful implementation of the FAM process will be the participation of Echelon II (and lower) from across the functional enterprise. Each FAM will meet process requirements for information gathering and consensus. The FAM will monitor the progress of the FAM Team/FAM Partnership Team as they execute the FAM Mid-Term Application and Database Rationalization Process.
- The designated FAM Lead develops and implements the process execution planning timeline with FAM approval.
- The FAM ensures that the FA has written vision, mission statements and objectives in place as a basis for analysis.
- The FAM ensures that the FA has written internal policies in place to guide the FAM Team/FAM Partnership Team on internal FA issues and decisions.
- The FAM cooperates in the identification and funding of required resources to support process execution. Additionally, the FAM assists in the identification of initiatives to help ensure that FA Enterprise application and database management is achieved within the FA and across the Enterprise.
- The FAM approves the progression of the FAM/Partnership Team through the major steps in FAM Mid-Term Application and Database Rationalization Process.
- Each FAM is responsible for controlling and assigning authorities and privileges to Echelon II commands, and is required to complete and maintain relevant sections of the ISF Tools/DADMS data-gathering tool.
- Each FAM is responsible for maintaining a relevant and accurate operational taxonomy in ISF Tools/DADMS. This is necessary to facilitate meaningful portfolio management decisions regarding the use of applications and systems to support specific operational activity requirements. FAMs are the final approval authorities for operational taxonomies and may modify operational taxonomies for their own functional areas only. As stakeholders, FAMs may make change recommendations to other FAMs for consideration and approval.

The DON CIO is expanding the functionality of the current Department of the Navy Application Database Management System (DADMS) to support the FAM application rationalization process. Each Echelon II command has representatives working closely with the FAM on their applications and databases. Developers and program managers who have questions about the FAM processes should contact their Echelon II Functional Area representative, or the FAM Lead.

3.2.3 Functional Data Manager (FDM)

The FDM is responsible for implementing functional processes to produce and monitor the use of data within and across functional activities, information systems, and computing and communications infrastructures:

- Assist PMs and other system developers in registering system/application (metadata) and data exchange formats and maintaining the metadata baseline.
- Develop and maintain Functional Area views of the Data Architecture.
- Develop candidate DoD standard data elements in coordination with the respective DoD Functional Data Administrator (FDA).
- Coordinate with applicable stakeholders to ensure that DoD proposed Data Standards are usable by Systems.
- Designate an authoritative data source for their respective functional areas and maintain the designation in the Application DADMS using processes and procedures approved by the CIO.

3.2.4 NMCI Designated Approval Authority (NDAA)

The DAA is a senior policy official who has the authority and responsibility to make the management decision to accept or not accept the security safeguards prescribed for an Automated Information System (AIS). The DAA is the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA is responsible for:

- Establishing and promulgating guidelines and security requirements applicable to the NMCI network and the software, which operates on that network.
- Assuring the fulfillment of system accreditation for his/her organization.
- Ensuring that AIS security mechanisms enforce security policy of the organization.
- NETWARCOM assumes the duties of Designated Approving Authority (DAA) for all operation, genser, Navy IT systems and networks. (See Naval Message in Appendix D22).

3.2.5 Program of Record (POR)

The POR is an office or individual who sponsors and has ownership responsibilities for an application. These responsibilities include but are not limited to funding and maintaining the application. The POR will conduct periodic reviews of their applications to determine if the application is current or requires a more detailed review and update. The POR, in conjunction with CDAs and FAMs, must develop a strategy to retire older, obsolete applications and conduct periodic reviews to ensure that only current applications are in service.

3.2.6 Central Design Authority (CDA)

For the purposes of this guide, a CDA is anyone (any organization, site, group, department, division, unit, section, individual, government, or government sponsored contractor) who desires to introduce a new application or change an existing application within the NMCI environment. CDAs are responsible for ensuring that their releases are compliant with Navy IA, boundary, and Group Policy Object (GPO) policies prior to deployment within NMCI. CDAs must work with the PORs and FAMs to develop strategies to retire older, obsolete applications and ensure that only current applications are in service. CDAs must keep in mind the requirements for developing and migrating applications that comply with

TFWeb, NMCI, Information Technology for the 21st Century (IT-21), Outside-Continental United States (OCONUS) Base Level Information Infrastructure (BLII) architectures, and DON standards.

CDA is also known as Central Design Activity, Central Development Activity, or Commercial Design Activity.

3.3 NMCI PROGRAM MANAGEMENT OFFICE (PMO)

3.3.1 Site Management Division, PMO (SMD)

3.3.1.1 Regional Classified Implementation Team

The PMO Regional Classified Implementation Team will work with the EDS regional classified rollout POCs in building regional schedules and clarifying regional issues. The PMO Classified Rollout Lead will work with the EDS lead, PMO CPMs and Regional Leads. The lead will ensure that a coordinated plan and comprehensive enterprise schedule is built and communicated to the customer.

3.3.1.2 Regional Organization

The Navy PMO and EDS have organized their field activities into 6 major regions: The NorthEast (NE), SouthEast (SE), NorthWest (NW), SouthWest (SW), Hawaii (HI), and Remote Site/RESFOR (RS) (refer to Appendix A). Note that these regional boundaries do closely match the Navy Regional boundaries; however, there are some cases where multiple Navy regions are mapped into one NMCI region.

3.3.1.3 Transition Organization

There are three levels of organization that will be used to manage the NMCI rollout across the Navy: Site, Region, and Enterprise. The Navy PMO and EDS will assign personnel to work at each level (refer to Figure 3-1 below). At the site level, EDS' team members include the Site Delivery Manager, Site Transition Manager, Project Coordinator, and multiple specialized support personnel. The Navy PMO will assign a Site Integration Lead (SIL) working in conjunction with Site Transition Execution Manager (STEM), Information Assurance Tiger Team (IATT), and Technical Government Representatives, as required. At the Regional level EDS will provide a Regional Delivery Manager (RDM) and Regional Transition Manager (RTM), and the Navy PMO will assign a Regional Integration Lead (RIL). Finally, at the enterprise level, EDA management and Navy PMO management will engage via a Joint Enterprise Command & Control Center (JECCC) in interaction with members of the Command Center Support Team (CCST). It is the vision of the JECCC and CCST to:

- Monitor, track, and facilitate mitigation/resolution of Enterprise level AOR and Cutover issues.
- Act on behalf of Navy PMO and EDS team members, as appropriate.

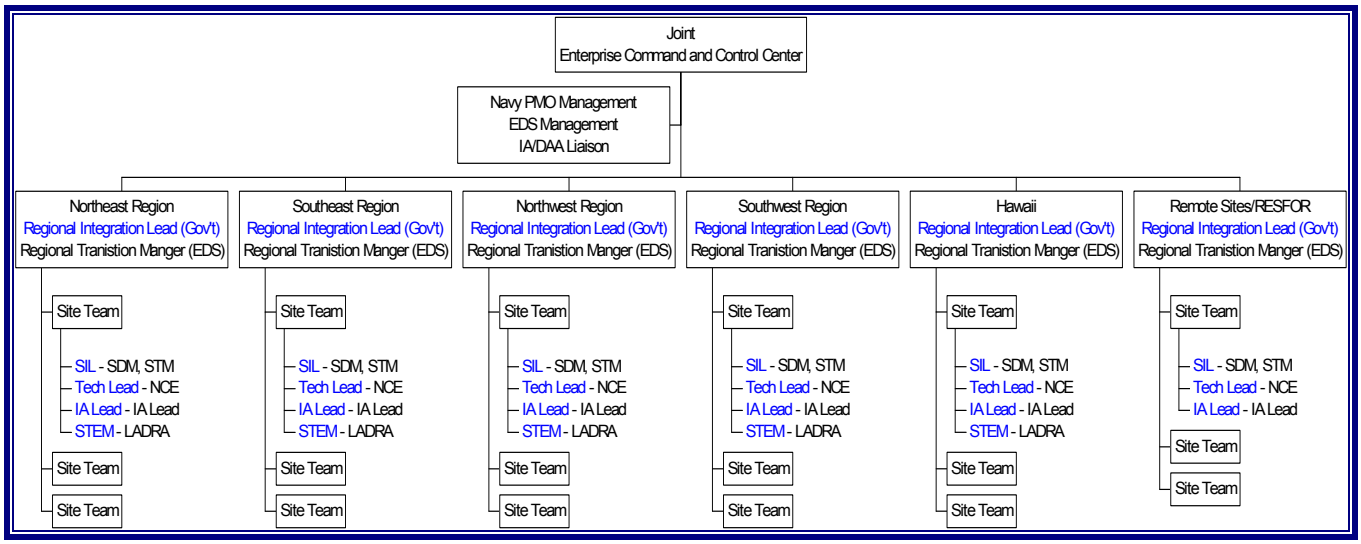


Figure 3-1. Navy PMO Joint Enterprise Command & Control Center (JECCC) Organization Chart

3.3.1.4 Enterprise Roles and Responsibilities

At the enterprise level, a JECCC will be established to provide a method for communicating critical issues from the sites and regions that could not be resolved at lower levels and need management attention to get resolved. The intent is to provide a central "one stop shopping" approach designed to provide enhanced support and improved resolution time to each region and site team. It is anticipated that the JECCC Support Team will meet weekly with each of the Regional teams to review status and take actions on open issues, which may impact AOR and Cutover schedules.

3.3.1.4.1 Government Enterprise

The following Navy PMO Personnel will participate as members of the JECCC Support Team:

- Program Management (PM) or Deputy PM
- Head, Site Management Division
- Head, Technical Solutions Division
- Head, Business Operations
- Legacy Applications Lead
- Information Assurance (IA) Lead/Designated Approval Authority (DAA) Liaison
- Issue Tracking Lead

In addition to the weekly joint reviews, the Navy PMO Joint Enterprise Command & Control Center Support Team will meet daily to review new issues and open actions.

3.3.1.4.2 EDS Enterprise

The primary responsibilities of the Deployment and Transition Manager are to oversee the readiness of sites to deploy and to direct deployment activities from an enterprise level.

3.3.1.5 Regional Roles and Responsibilities

At the regional level, the joint Navy PMO/EDS team will meet daily to assess work efforts and issues as well as track progress according to schedule.

3.3.1.5.1 Government Regional Integration Lead (RIL)

The RIL is responsible for each site within the assigned area of responsibility and performs as the direct liaison between Navy NMCI PMO, EDS Regional personnel, and Flag/Executive Level Claimant Representatives in matters of issue mitigation and resolution. Specific RIL functions include but are not limited to:

- Identifying each customer site within area of responsibility.
- Interacting on a daily basis with the EDS Regional Managers.
- Interacting with each site manager *on a daily basis* to facilitate positive 2-way communications.
- Developing, maintaining, and monitoring project site schedules and critical milestones and working mitigations to prevent schedule slippages.
- Monitoring and reviewing Government deliverable schedules.
- Ensuring that all Government deliverables are delivered on time and within project scope.
- Developing, managing, and close monitoring of regional roll-up schedule derived from individual site lead schedules.
- Assignments and management of all regional resources, including Technical Representatives, STEM, and IA/IATT.

3.3.1.5.2 EDS Regional Transition Manager (RTM) & Regional Delivery Manager (RDM)

The primary responsibility of the Regional Delivery Manager (RDM) is to oversee end-to-end delivery on a regional level. The RDM manages each of the Site Transition Managers (STM) within their geographic region.

The primary responsibility of the RTM is to oversee and manage all Site Transition Managers within their region. Duties include overseeing schedule and project plan compliance, and problem escalation and resolution. Regional Transition Managers report directly to the Deployment and Transition Manager.

3.3.1.6 Site Roles and Responsibilities

The *Joint Site Management Team* is by far the most critical team for the successful implementation of NMCI. The site team is responsible for making NMCI happen, for rolling seats, and making sure that NMCI works for our customers. It is therefore critical that our site Navy PMO and EDS teams work together in a spirit of cooperation and teamwork to allow for the successful completion of common goals. It is expected that our joint site teams will be working together on a daily basis to ensure good communication and synchronization of efforts.

3.3.1.6.1 Government

The Government segment of the site team will include a Site Integration Lead (SIL), at a minimum, but may also include a technical representative, STEM, and IATT. It will be up to the RIL, working closely with the SIL, to determine what resources are required for each site.

3.3.1.6.1.1 Site Integration Lead (SIL)

The SIL is a government PMO representative to the Command/Site in all matters pertaining to the NMCI transition. They are an on-site PMO representative who conducts daily and weekly reports to the CPM, explores granularity of issues, ensures site allocation of resources, etc. The primary mission of the SIL is to assist the Command/Site in their transition to NMCI.

3.3.1.6.1.2 Customer Technical Advisor (CTA)

The CTA is a PMO site and region representative who is responsible for working technical issues associated with architecture, reach-back, Community of Interest (COI), Science &Technology (S&T) seats, and other site unique requirements.

3.3.1.6.1.3 Site Transition Execution Manager (STEM)

The STEM is a regional on-site PMO representative who assists with the initial parts of the transition. The STEM assists multiple sites at a time. The STEM is involved with Identification and Rationalization, Collection, Media Submission, Certification and Testing processes (all of these processes are explained in Section 4.0 of this document). STEMs assist and give guidance to the site during these processes to prepare the site for the remainder of the transition. The STEM primes the site for the ISF teams who will transition the site.

To prepare the site for transition, the STEM:

- Assists the site with completing the Final Rationalized List on time
- Assists with the collection and submission of RFS & Media
- Assists in scheduling of personnel for Point of Presence (PoP)-in-a-Box (PIAB) / Legacy Application Deployment Readiness Activity (LADRA) testing
- Provides education/training on how to conduct:
    - Application mapping
    - Peripheral listing and mapping
- Works with Site on any issues reflected in the ISF Tools Database
- Acts as a liaison between ISF and Command/Site Legacy Application Point of Contact (LAPOC)

Once the STEM has properly prepared the site for ISF to continue transition, the STEM moves on to other sites to assist them as the program executes.

3.3.1.6.1.4 Information Assurance (IA)/IA Tiger Team (IATT)

The IA is a PMO site and region representative is responsible for working IATO/IATC issues along with classified network issues such as Protected Distribution System (PDS). The IATT is a PMO site and region representative who is responsible for assisting in the testing and accommodation of site mission critical applications. The IATT will also assist in working with the appropriate Functional Area Manager (FAM)/Designated Approval Authority (DAA) authorities to grant permission to operate certain ports and protocols on the NMCI network. In many cases, the site IA and IATT will be the same individual. The IATT representatives are assigned to support a region. The IATT representative reports directly to the RIL. IATT has three primary tasks: Regional IATT support, Quarantine Remediation, and Quick Look Assessment.

3.3.1.6.2 Electronic Data Systems (EDS)

The EDS segment of the site team will include a Site Delivery Manager, Site Transition Manager, and Project Coordinator (PC), at a minimum, but may also include additional EDS support as required to ensure adequate coordination and support of AOR and Cutover requirements.

3.3.1.6.2.1 Site Delivery Manager (SDM)

The primary responsibility of the SDM is to be the overall manager of all site activities at the base level. The site manager is responsible for the management of legacy networks from AOR through cutover and for base level management of the NMCI network including Service Level Agreement (SLA) compliance. As the senior delivery manager at the site level, the site manager is ultimately responsible for insuring a smooth transition to NMCI.

3.3.1.6.2.2 Site Transition Manager (STM)

The primary responsibility of the STM is to provide hands-on project management of all aspects of NMCI seat delivery. The STM performs as the transition manager on site from AOR through cutover and is responsible for developing, executing, and maintaining a project plan leading to the on-time and within budget deployment of NMCI seats at designated locations. The STM oversees and coordinates the scheduling and delivery of all infrastructures, including cable plant, security firewalls, and wide area network connectivity, and provides the site interface for all design and approval activities. The site manager in support of the customer helps develop a cutover schedule facilitating an orderly transition to NMCI. The STM reports directly to the Regional Transition Manager (RTM).

3.3.1.6.2.3 Project Coordinator (PC)

The Project Coordinator (PC) also works at the site level and is responsible for keeping the Project Site Schedule (PSS) up to date, entering Issues, Risks, Actions, Assumptions, Decisions (IRAAD) issues and Schedule Change Requests (SCRs). The PC is the only site representative with writes access into the PIV tool. The PC accepts schedule and IRAADs input from both EDS and Government PMO representatives. The PC must ensure that they receive input from both parties prior to entering data into PIV. If there is differing opinion on schedule status or issues, the PC must enter both perspectives into PIV so that it may be reviewed and acted on by senior PMO/EDS management.

EDS coordinates a weekly NMCI Regional Status VTC with the PMO to discuss and resolve Site/Claimant issues. If a Site Cutover is impacted due to a legacy application issue, the issue is generally reported via the IRAAD.

SCRs submitted by the PC are forwarded to the Schedule Change Control Board (SCCB) for review and approval.

3.3.2 Legacy Systems Division, NMCI PMO

Provide technical resources:

- To Legacy Application readiness through oversight during transition and liaison with EDS and Legacy Applications POCs.
- For data management through testing and Quarantine of applications.
- And assist with the development of policies and procedures for Risk Mitigation strategies.
- To coordinate and provide guidance for Enterprise applications being introduced into NMCI.

3.3.2.1 Enterprise Application Group for Legacy and Emerging (EAGLE)

The Navy PMO created the EAGLE Team, which has three main purposes:

- To provide resources that will focus on the Critical Joint Applications (CJAs) listed in the NMCI contract.
- To provide resources that will focus on the CDA, POR, or PM owned applications, with the intent of certifying applications once at the enterprise or developer's level rather than re-testing and certifying applications at each individual site.
- To provide resources that will focus on collecting all application related information and provide the focal point for the Site Solutions Engineering (SSE) teams for this information.

The EAGLE Team is divided into three sub-teams:

3.3.2.1.1 Claimant CDA Support (CCS)

The CCS is focused on educating CDAs/PORs on architecture requirements for developing and deploying applications in NMCI. In addition, this team will provide guidance in the collection and submission of Engineering Review Questionnaires (ERQ), software media, and CDA RFS documentation for CDA/POR applications. The end-goal is to produce an enterprise version of each appropriate application and make it available for selection in the Application Catalog in the ISF Tools Database.

3.3.2.1.2 Data Management Team (DMT)

The DMT is tasked with maintaining the ISF Tools Database as the "data repository" for all applications deployed in NMCI. This team oversees accuracy and data integrity, and maintains consolidated application data in one central and accessible location. The team provides tool configuration, data cleanup, and maintenance. It also supports all levels of users throughout all steps of the transition process and the CDA submission process. One of this team's primary goals is to reduce the amount of rework required by the CDAs/PORs and by each site team as they come across applications that have been previously encountered.

3.3.2.2 Information Assurance Tiger Team (IATT)

The NMCI IATT, under the direction of NMCI PMO and NETWARCOM, is a government team consisting of government (civilian and military) and contractor personnel providing technical leadership and IA expertise to government and EDS representatives migrating Legacy Applications into NMCI. It is the responsibility of this team to ensure that the associated residual risk of Legacy Applications to NMCI is understood and minimal. The primary objectives of the IATT are as follows:

- Act as an impartial agent of the NMCI DAA and NMCI PMO to ensure that Legacy Application migration solutions adhere to acceptable security practices and do not significantly impact Legacy Application operational capabilities.
- Raise the IA awareness of Legacy Application owners, developers, implementers, and users through professional consultation, presentations, workgroups, and relationships with other Legacy Application related teams.
- Ensure that the end-state posture of NMCI is not significantly diminished due to the introduction of Legacy Applications into NMCI.
- Provide expertise, guidance, and execution oversight of the Risk Mitigation Phase process of Quarantine Remediation.

The IATT will be responsible for performing the following functions:

- Provide Legacy Applications IA education to claimants, sites, users, and developers. Many of these efforts will be coordinated with the PMO Site Visit Team.
- Provide Legacy Applications IA consulting to the PMO Customer Project Managers. In this role, IATT will act as a single conduit for the CPM regarding Legacy Applications IA.
- Identify, in conjunction with each claimant, the prioritization of legacy applications. This prioritization will be referenced when performing analysis and assigning resources to complete Quarantine Remediation processes.
- Develop, refine and implement the Quarantine Remediation process.
- As part of the Quarantine Remediation process, participate with government leads in on-site Legacy Application reviews, complex Legacy Application reviews, and the development of Legacy Application transition strategies.
- As part of the Quarantine Remediation process, work with sites to submit requests for modifications or exceptions to NMCI firewall security policies.
- Develop (publish) Systems/Server Migration guidance. Develop strategies and work with site in this effort.

3.3.2.2.1 Quick Look Assessment Team (QLAT)

The Quick Look Assessment Team (QLAT) is responsible for conducting Information Assurance assessments on legacy networks connected to NMCI. The overall objectives for the QLA are twofold:

1. Determine the acceptable level of risk for legacy networks connected to NMCI.
2. Reduce the number of legacy networks that have transitioned to EDS under Area of Responsibility (AOR) in NMCI. These objectives support the implementation of the

Transitional B2 Firewall Policy, and aim toward a reduction in both legacy applications and dual desktops. Additionally, the QLA supports the legacy system transition.

The QLAT conducts scans and technical network assessments over a five-week period. These assessments include "mitigation of major vulnerabilities leading to a recommendation for IATO/ATO." A final report is published for the Site to provide recommendations for use in the Risk Mitigation and Systems Transition phase. There will be a total of five QLA teams, each team assigned to a region.

3.4 CLAIMANT

3.4.1 Sponsoring Echelon II Command

An Echelon II Command or claimant is defined as an activity that reports to CNO or higher as a normal part of operations. The Echelon II Command is responsible for exercising application management over all subordinate units or organizations. The Sponsoring Echelon II Command is defined as the parent organization of the POR and CDA. As the parent organization, the Sponsoring Echelon II Command provides program and content oversight of the applications and releases. The Sponsoring Echelon II Command plays a review and approval role in the Release Deployment Process.

3.4.2 Customer Project Manager (CPM)

The CPM is a government PMO representative to the Echelon II Command/Site in all matters pertaining to the NMCI transition. They are a direct liaison between the NMCI PMO and Flag/Executive Level Claimant Representatives in matters of mitigation and resolution. The CPM's primary mission is assisting the Echelon II in the management and execution of the transition of their Commands/Sites. CPMs may, at their discretion, escalate unresolved legacy application issues up to the RIL for resolution.

3.4.3 Contract Officer's Representative (COR) or Contractor Technical Representative (CTR)

A government representative of the Command/Site who oversees the NMCI transition for their respective Commands/Sites. Provides government technical interface with EDS and monitors compliance with NMCI contract requirements.

3.4.4 Legacy Application Point of Contact (LAPOC)

The LAPOC is the customer's primary POC for all Legacy Applications transition issues at their Command/Site. The POC works closely with the EDS and PMO to implement NMCI transition.

Customers must identify a primary POC for all Legacy Applications at their Command/Site prior to Cutover -180. The LAPOC should be comfortable communicating with people, knowledgeable about the Command's/Site's IT resources, and familiar with simple databases. The POC works closely with EDS and PMO to implement NMCI transition.

As the primary site representative for the Legacy Applications transition process, the LAPOC is responsible for:

- Preparation of the site for Legacy Applications Transition.
    - Coordinate with the STEM, EDS SM, and other Legacy Applications transition personnel (the STEM and EDS SM are discussed later).

  - Review this guide completely and be familiar with its content.
  - Obtain access to ISF Tools Database.

- Lead Identification and Rationalization effort.
  - Create the Identification and Rationalization Game Plan.
  - Conduct user surveys for COTS and GOTS requirements.
  - Maintain Command/Site's ISF Tools Database entries.
  - Deliver Final Rationalized List no later than Cutover –120.
  - Create and deliver Application Mapping no later than Cutover –120.
  - Develop and deliver rationalized Peripheral and Driver List.
  - Identify Legacy Applications Servers.
  - Identify datashares and reachback requirements.
  - Create site Loadsets.

- Lead the Collection efforts.
  - Identify Licenses.
  - Identify desktop and server connectivity (Network Diagram).
  - Collect Media and supporting documentation in preparation for Submission.
  - Lead media submission efforts.
    - Submit media and supporting documentation to on-site EDS SM
  - Coordinate Certification, Testing, and Pre-Deployment Efforts.
    - Schedule and ensure application owner participation in the testing processes.
  - Coordinate post-migration application issues.

3.4.5 Application Owner/User

Application Ownership – every identified application will have a designated owner. That owner will either be a formal CDA, a POR, or a FAM. If no owner for an application is identified, the application will not be allowed to migrate to NMCI and any reference to it will be removed from ISF Tools Database.

The application owner/user may be asked to come to the test area to participate in usability tests to verify that an application is working properly and that it can access the server, datashare, or Web site as required.

3.5 ELECTRONIC DATA SYSTEMS (EDS)

3.5.1 Site Manager (SM)

The EDS SM is the lead EDS member at each site. The SM is responsible for the delivery of all NMCI services at the designated location. Service delivery roles include:

- "As-is" support during the AOR period.
- Migration/transition support during the Cutover period.
- Post Cutover daily production support of existing and new Navy requirements.
- Coordinate EDS operations for the site.
- Will remain on site for postproduction.
- Liaison to government POCs (CTR).
- Maintains schedule of EDS initiative.

3.5.2 Product Delivery Manager (PDM)

The PDM is an EDS resource that works in concert with the EDS SM, to plan, assist, coordinate and execute the delivery of EDS and Government application requirements. The PDM serves as Legacy Systems' resource and delivery manager for claimants and sites they are assigned to. The PDM will provide the solutions that aid in the successful migration of applications and systems to NMCI. The roles and other information on PDMs are discussed below.

The PDM serves as Legacy Systems' resource and delivery manager for claimants and sites they are assigned to. This includes:

- Planning, tracking, deployment, and delivery of those resources, products, or activities that directly support processing of applications and systems migrating to NMCI.
- Serving as the SME for the Legacy Application processing, Legacy Application customer processing, and SSE Team training, planning and deployment.
- Supporting the EDS SM and Claimant Manager to ensure that EDS Legacy Systems activities support the sites in the migration of applications and systems to NMCI.
- Assisting with the requirements for delivery of applications and the transition of the sites to NMCI.
- Ensuring that the sites and other EDS teams are prepared to deliver their requirements in support of site rollout.
- Planning, deploying, and managing resources, tools used for testing, documenting, and delivering applications, and systems for NMCI Rollout.
- Working closely with the site-appointed LAPOC to resolve issues.

PDMs have two main deliverables:

- Site and Resource Deployment Plan - In this plan, the PDM specifies the steps to get the site to Cutover (AOR +60).
- Weekly DAA Summary - This summarizes the progress the site has made with LADRA testing and reports the application's LADRA results. LADRA will be explained later in Section 4.8.1.

3.5.3 Product Delivery Analyst (PDA)

To assist the PDMs with the numerous tasks they have, each PDM is assigned a PDA. PDAs are physically located at the EDS Commerce Point facility in San Diego. They provide Legacy Application data and other information for management reports, which rely on information extracted from the ISF Tool Database. The PDA provides process support on the submission of Legacy Applications, training, ISF Tools support, data analysis and progress reporting.

PDMs and PDAs will continue to work with a site after Cutover is complete to make sure that the transition is complete and went well.

The EDS PDA is an advisory POC to back up and support the EDS PDM. The PDA provides process support on the submission of Legacy Applications, training, ISF Tools support, data analysis and progress reporting. In addition, the PDAs work with on-site SSE Teams to ensure readiness of applications and associated documentation prior to and during testing. The PDA also works with all

members of the Legacy Applications Transition team to ensure that proper documentation standards are kept. PDAs interface with government and EDS personnel, including (but not limited to): STEM, PMO, NADTF, DMT, PEO-IT, PDM, SSE Team members, SM, Customer Technical Representative (CTR), LAPOC, AIT, EAGLE and IA Teams. PDA responsibilities include:

- Review, analyze and provide documentation on LADRA readiness and Rationalized List status for the Pre-AOR Review.
- Create reports for PDMs and EDS Legacy Applications management.
- Identify applications submitted that already have a documented NMCI solution (Certification by Association (CBA)).
- Provide process guidance and some limited ISF Tools training to EDS and Navy personnel on the submission of Legacy applications and peripherals.
- Investigate media and documentation issues (RFS, etc.).
- Participate in recurring site status meetings to provide support and problem resolution.
- Conduct Readiness Review (RR) and Post Cutover Assessment (PCA) to ensure readiness of site applications and final status.
- Classified PDA is primary POC for creation of Classified Site Workbooks.
- The Classified PDA is the EDS POC for all Classified Rationalized Lists.

3.5.4 Site Solution Engineering (SSE) Team Base Lead

The SSE Base Lead is the senior member of the team who coordinates team activities and provides assistance to the SM. The SSE Lead will serve as the on-site representative and spokesman for the team, as well as ensuring that any reporting requirements or deliverables are met. Besides serving as Base Lead, this individual will also review the team's deliverables and ensure the integrity of the data and solutions for each application. The SSE Lead is responsible for:

- Interfacing with site STEM and LAPOC (or the designated Legacy Applications representative) to maintain a loaded queue of POCs to support on-site testing (PIAB, Local Deployment Solution Development and Testing (LDSD&T) or LADRA) activities, when required.
- Analyzing Site/Claimant-provided list of priority applications for strategic targeting and logical assignment throughout the team.
- Monitor team activities and productivity to ensure that throughput is optimal and take corrective actions if levels drop below required threshold.
- Give guidance and assist the PDM in managing the on-site testing resources to ensure adequate support of team activities.
- Provide, update and review daily/weekly reports and team deliverables. Update Project Plan.

3.5.5 Site Solution Engineering (SSE) Team Member

The SSE Team Member is responsible for conducting Legacy Application on-site analysis and testing. The SSE Team Member will be assigned Legacy Applications by the SSE Base Lead, and will be required to process them according to defined procedures and provide Application Deployment Solutions (ADSs). Besides processing Legacy Applications, the SSE Team Member will be required to update the SSE Base Lead daily on status changes for all assigned applications. The SSE Team Member is responsible for:

- Reviewing any available documentation (existing ADS from other sites, POC provided documentation, etc.).
- Executing the on-site testing (PIAB, LDSD&T or LADRA) as outlined in current process documentation.
- Completing an ADS, and providing Base Lead with connectivity, GPO, Network Address Translation (NAT), Domain Name System (DNS) or other requirements for deployment.

3.5.6 Application Integration and Testing (AIT) Team

The AIT Team is responsible for packaging and NMCI Certification testing of Enterprise applications, emergent (new) applications, and updates/upgrades/patches/fixes for existing applications. CDAs or an EDS Site Team (Site Solution Engineering Base Lead or Site Transition Manager) are responsible for providing media to the AIT Team for packaging. The AIT Team is responsible for these functions and responsibilities at the San Diego Certification Lab, and the Classified Lab at the San Diego NOC;

- Auditing of applications for compliance with the NMCI Ruleset.
- Packaging of applications for deployment.
- Certification of applications for deployment.
- Deploying package to the Novadigm Radia Servers.

4.0 RAPID CERTIFICATION PHASE

Figure 4-1 depicts the Rapid Certification Phase process from start to finish. Notice the legend at the bottom right side of Figure 4-1; the colors in the legend correspond to ownership of primary responsibility for completion of the process. For example, the "Media Submission" box is blue, and represents a Government/Site responsibility for completion. Note that many of the processes are tan, indicating a joint responsibility for completion shared by EDS and the Government.

The overall goal of the Rapid Certification Phase is to work with EDS to ensure that the right applications are available to the right people on the right NMCI seats. This goal ensures that the DON can complete this mission and business in a timely manner. From the customer's perspective, this means many things, including:

- Understanding who uses particular applications at the site.
- Understanding what version(s) of an application are in use at the site.
- Communicating with EDS and PMO personnel to help them understand the applications.
- Communicating with Echelon II NMCI personnel as lists of needed applications are reviewed.
- Making the resources available to accomplish the processes.

Classified Legacy Application

Classified Legacy Application Transition typically follows the steps of the unclassified process described below. The Classified Legacy Application Transition is described in detail in Appendix F.

A segway is needed here…Next we look at the first process within Rapid Certification, Site Preparation.

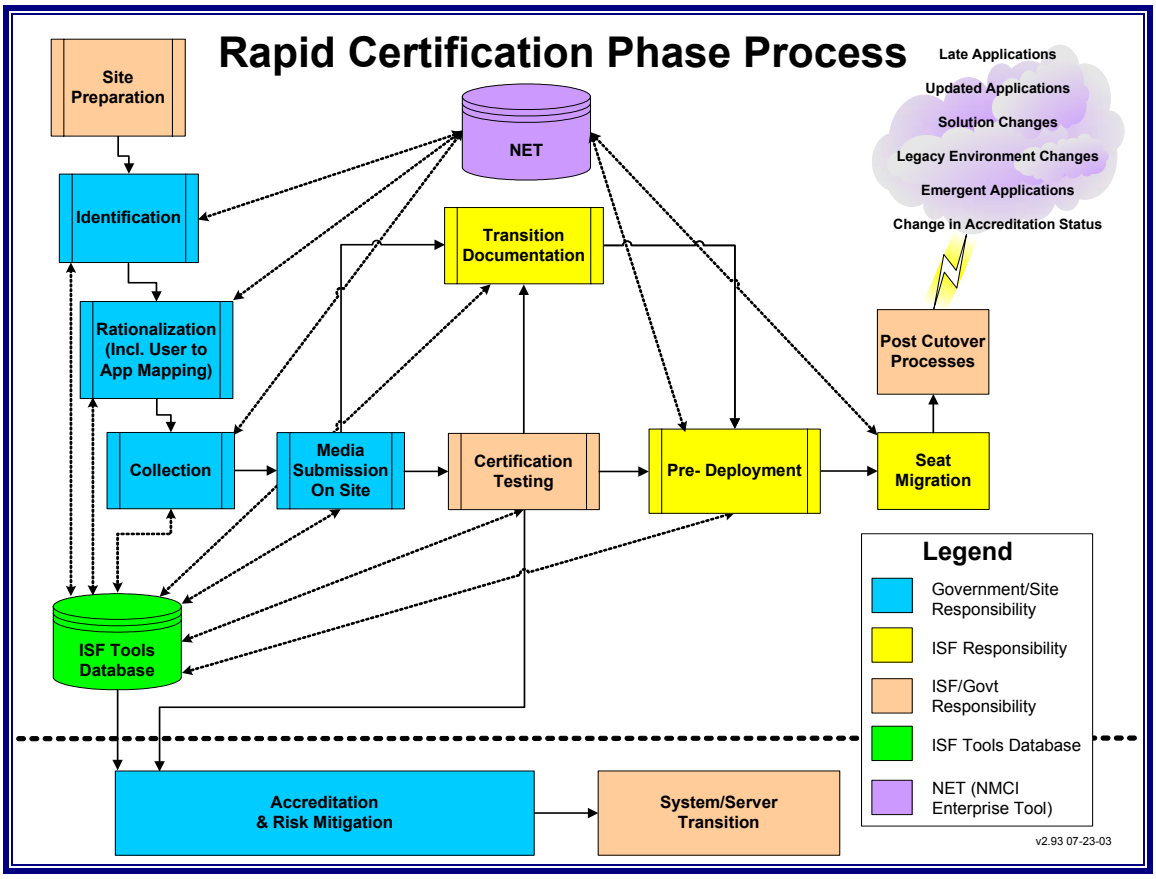


Figure 4-1. Rapid Certification Phase Process

4.1 SITE PREPARATION

Figure 4-2 depicts the details of Site Preparation from the NMCI customer perspective. The activities are designed to get a site ready to start the transition process well before any contractor or Government program management personnel are involved. Lessons learned have shown that Sites that do not wait for the EDS & PMO Personnel to arrive do not jeopardize the cutover date.

The first step in starting a successful transition is for the Command's NMCI Transition Team to obtain the Legacy Applications Transition Guide (LATG). Each member of the team should become fully familiar with all the key transition activities and deliverables. The education of the Transition Team is not a lone venture. As transition progresses at the Site, many members of the PMO and EDS will further assist in training and completion of Command Deliverables. At a minimum, the Commanding Officer (CO), the IT manager on the CO's staff, the CTR, and the LAPOC should all have copies for reference. Customers should read and understand the overall NMCI Transition processes, which can be found at the following URLs:
http://www.nmci-isf.com/transition.htm and/or
http://www.nmci.navy.mil/Primary_Areas/Transition_to_NMCI/Index.htm

As part of the site preparation, the following actions need to be accomplished:

- Appoint LAPOC.
- Identify Classified Requirements.
- Establish contact with PMO and EDS.
- Establish ISF Tools Database access.
- Obtain the ISF Tools Database Users Guide.
- Determine facility Requirement for EDS Testing.
- Acquire local IATO for testing connectivity.
- Review, accept and assign facilities.

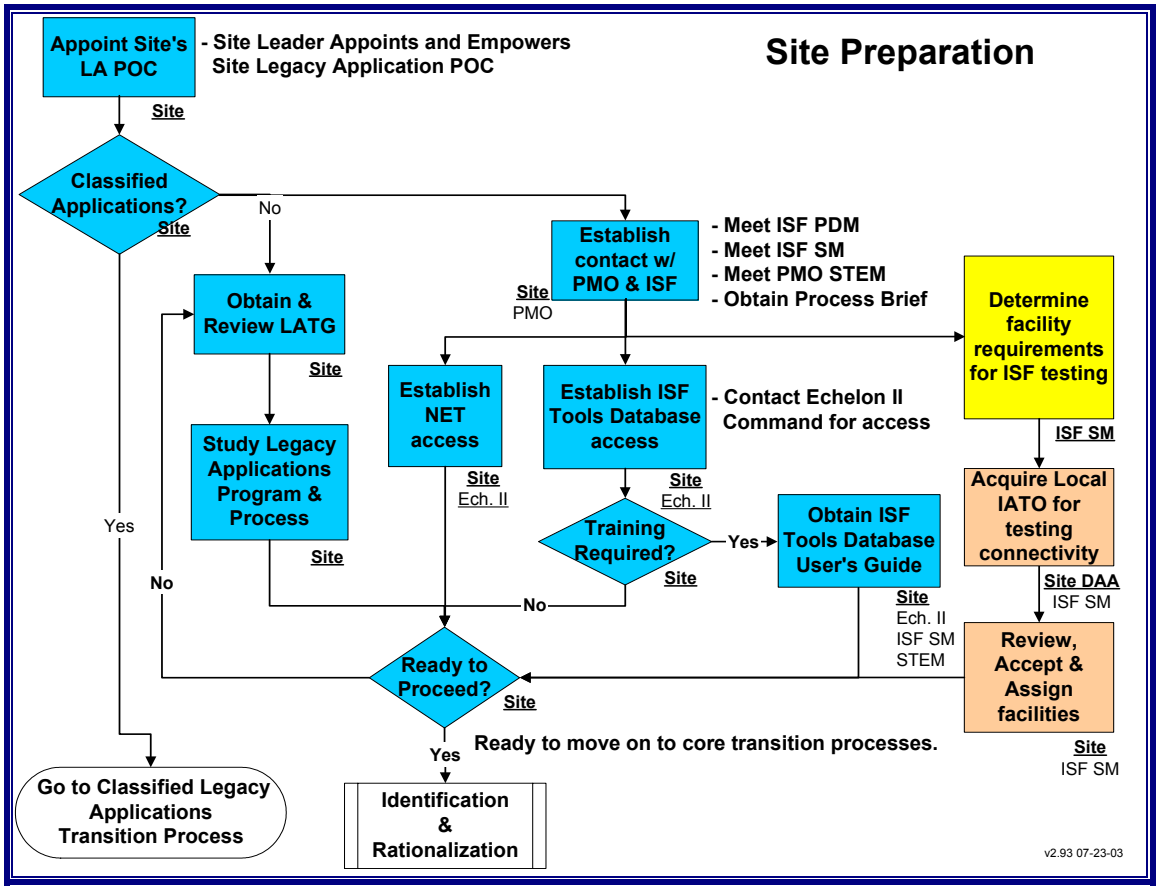


Figure 4-2. Site Preparation

4.1.1 Appoint Legacy Application Point of Contact (LAPOC)

The Site must identify a primary POC for all Legacy Applications at their Command/Site. This LAPOC is knowledgeable of the Command's/Site's IT resources and familiar with simple databases. The POC works closely with the EDS and PMO to implement NMCI transition.

4.1.2 Identify Classified Requirements

The Site determines whether or not it has any classified applications. If the Site contains classified application, then the Site is required to perform the Classified Legacy Application Transition process,

which can be found in Appendix F. If the Site determines that the application is Unclassified the Site follows the Unclassified Legacy Application Transition Process. A Site with both unclassified and classified applications will work both processes, which can be worked simultaneously.

4.1.3 Establish Contact with PMO and EDS

The Site will contact the appropriate PMO and EDS Team Members to begin transition of Legacy Applications into NMCI.

- Site Integration Lead (SIL) (Section 3.3.1.6.1.1)
- Site Transition Execution Manager (STEM) (Section 3.3.1.6.1.3)
- Electronic Data Systems (EDS) Site Manager (SM) (Section 3.5.1)

4.1.4 Obtain ISF Tools Database Access

The Site should contact their appropriate Echelon II Command to obtain access to the ISF Tools Database. Use of this database is mandatory and is critical to a Site's successful application transition effort. All Echelon II Commands have the authority to create user accounts in the ISF Tool Database for their subordinates. To obtain an account, select the User *Access Request Form* at the following URL: https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp.
User requests may be submitted for Navy, USMC, or EDS personnel

4.1.5 EDS Database Training

If training is required on the use of the ISF Tools Database, the Site should begin by obtaining the ISF Tools Database User's Guide. The User's Guide is available at the following URL: http://www.nmci-isf.com/transition.htm Additional training is available through Echelon II POC, by contacting the EAGLE DMT (nmci-pmo-isftdb@spawar.navy.mil), or by contacting the NMCI Help Desk at 1-866-THE-NMCI.

4.1.6 Determine Facility Request for EDS Testing

The EDS SM consulting with the site determines which facilities will be used for testing the Legacy Application. Customers must identify a suitable location to accommodate a PIAB or NMCI Test Seat. The PIAB is a "mini-NMCI environment" used by the EDS to identify application characteristics. The NMCI Test Seat is an actual NMCI seat used when the NMCI base infrastructure is in place. Deployment of a PIAB or NMCI Test Seat to a site comes later in the transition process, but a prudent site prepares facilities, makes network access arrangements, and understands power requirements in advance of the testing environment's arrival. Further information on the PIAB and NMCI Test Seat can be obtained by contacting the EDS SM and SSE Teams.

4.1.7 Acquire Local IATO for Testing Connectivity

The EDS SM works with the Site's DAA to obtain authorization to connect the NMCI PIAB or the NMCI test seat to the Legacy Environment through the NMCI Network. This IATO is for connectivity of hardware and networks and does not pertain to operation of Legacy Applications. This IATO is obtained via the Site and the EDS Network personnel.

4.1.8 Review, Accept and Assign Facilities

EDS creates a Site Facilities Plan that includes recommended square footage, power requirements, environmental requirements, and cable requirements as well as computer hardware. The plan is provided

to the site for review and acceptance. Negotiations between EDS and the site may occur. Once the Site and EDS reach agreement, the Site Facilities Plan is implemented. Additional information on Government-Furnished Facilities may be obtained at this URL:
http://www.nmci-isf.com/transition.htm#GovCheck

4.1.9 ISF Tools Database

The ISF Tools Database has been developed to record and share collected information about software applications to be deployed in NMCI. It is the authoritative source for all Legacy and Emerging Applications in NMCI. Naval Message D.2 provides amplification on the tool. ISF Tools will collect all information related to Legacy Applications Transition, specifically:

- Site Preparation
- Identification
- Rationalization
- Collection
- Media Submission
- Testing – Packaging and Certification
- LADRA test results and Quarantine status during Pre-Deployment

The ISF Tools Database is also the authoritative source for testing and deployment information for Legacy Applications, where users can:

- Record all of their Legacy Applications.
- View Application Catalog.
- Develop their list of Legacy Applications and submit their Rationalized List.
- Create a RFS for Legacy Applications.
- Monitor real-time status of Legacy Applications proceeding through the transition process.
- Create reports such as a site's Workbook showing all rationalized Legacy Applications and their status in NMCI.
- View NADTF and FAM approval status.
- View Application waiver status.
- Identify and track Quarantined applications.
- View RFS Notes on application issues and solutions.

Further information on the ISF Tools Database is available online at the following URL:
http://www.nmci-isf.com/transition.htm

4.1.10 DON Application and Database Management System (DADMS)

The DADMS tool was created to provide the FAMs with the following capabilities: segregate applications by function; identify and catalog application attributes, manipulate information related to applications, and facilitate the reduction of applications to a minimum number needed to support the operation of the Navy IT enterprise. To enhance the Navy's success in effectively implementing NMCI, the CNO established a goal to reduce Navy Legacy Applications by 95 percent within one year or by May 2003. To accomplish this effort, the DON CIO has directed the development of the DADMS to support the FAMs and FDMs in developing standard applications, databases, and data elements. This effort will provide structure to maintain configuration control of all applications and databases across all DON networks. This will facilitate the integration process to capture both the Navy and Marine Corps existing

IT business rules and requirements. Processes and procedures can be found on the DADMS website under the policy and guidance link: https://www.dadms.navy.mil/.

4.1.11 Site Ready to Proceed Core Transition Processes

Once the transition team and tools resources have been established: processes are in place, the Site Plans have been completed, and then the Site is ready for Identification and Rationalization.

4.2 IDENTIFICATION

Figure 4-3 depicts the Identification process. The goal in Identification is to inventory all Legacy Applications required to conduct business after transition to NMCI. The Identification and Rationalization processes are important Government responsibilities. While the Echelon II Commands are responsible for oversight of these steps, much of the execution occurs at the operational or site-level. Experience with early site implementation confirms the value of being proactive. The first increment customer that sites should begin these processes well in advance of 180 days before Cutover. The lesson learned is that the Site should not wait for EDS or PMO personnel to arrive on-site for this work to begin.

As part of the Identification process, the following steps need to be accomplished:

- Create the Identification and Rationalization Game plan.
- Socialize Site's Game Plan and Strategy.
- Concurrent Processes.
- Survey users for GOTS requirements.
- Survey users for COTS requirements.
- Create user list and begin Application Mapping.
- Create Site Loadsets.
- Gather in use Peripherals and Drivers.
- Identify Legacy Applications Servers.
- Identify Datashare and Reachback requirements.

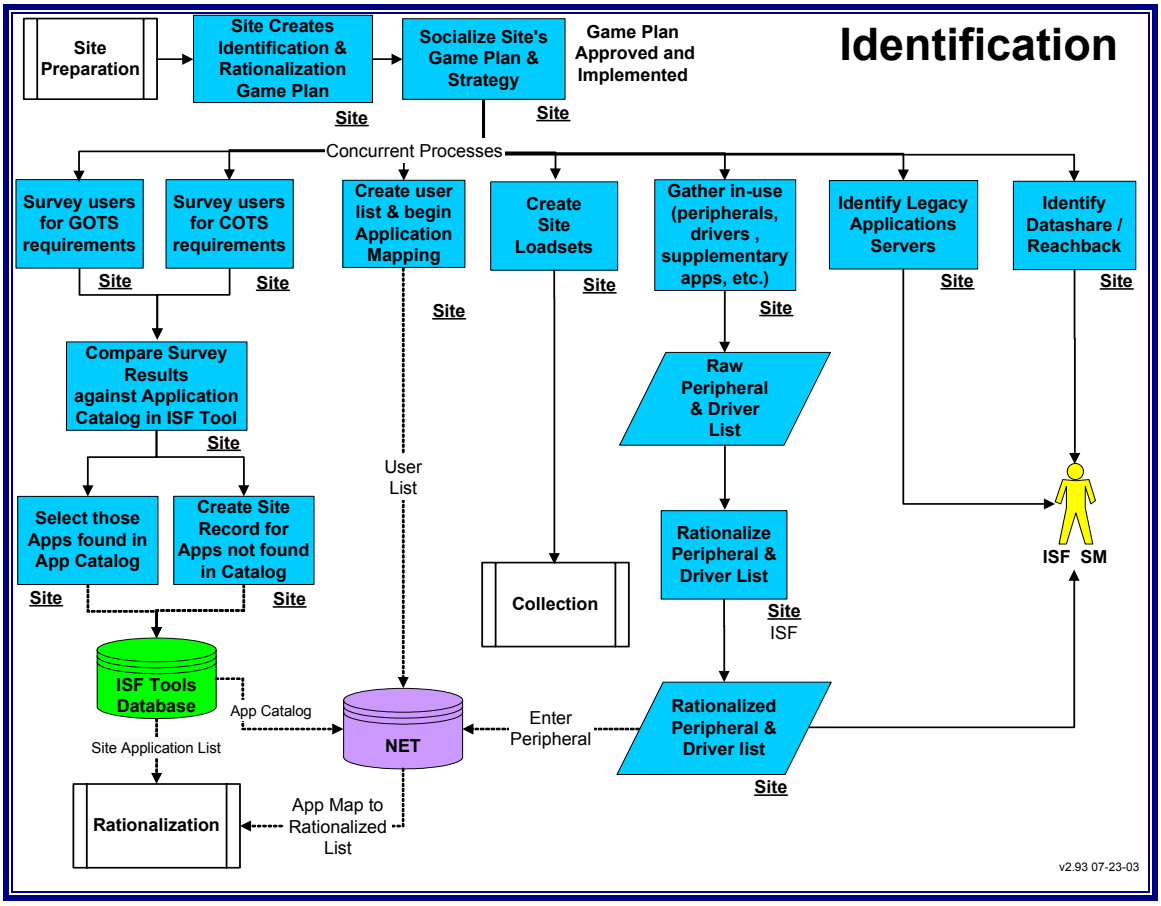


Figure 4-3. Identification

4.2.1 Create the Identification and Rationalizing Game Plan

Customers should create and implement an Identification and Rationalization "Game Plan." This plan specifies who at the site is responsible for each of the tasks associated with the identification of Legacy Applications, as well as other critical information related to NMCI transition. There is no set format or template for the site's game plan. The key individuals selected by the site must meet, communicate, and formulate a viable plan that can be easily coordinated and implemented.

Once the plan is implemented, numerous types of information will be identified. . This will include:

- Identification of the GOTS applications that will be required in NMCI.
- Identification of the COTS applications that will be required.
- Identification of the of mission essential website URLs used by the site.
- Creation of the initial Application Mapping list.
- Identification of desktop legacy peripherals, drivers, and associated software.
- Identification of the Legacy Application servers.
- Identification of the Datashare and Reachback requirements for the Legacy Applications.

4.2.2 Socialize Site's Game Plan and Strategy

Once the Command/Site has created a game plan and strategy for identifying and rationalizing Legacy Applications, the plan will be socialized among the appropriate staff.

4.2.3 Survey Users for GOTS/COTS Requirements

The LAPOC at the customer site will ensure that a survey is conducted for the GOTS and COTS operational requirements. All users should be surveyed to determine their COTS and GOTS requirements. There is no set procedure, format or template for conducting this survey. Each Command/Site must develop methods based on their needs. Tools such as Altiris Asset Management Suite, Microsoft SMS and Belarc advisor are examples of tools commercially available to automate the process. Once the application requirements are collected and compiled, they are entered into the ISF Tools Database.

4.2.3.1 Entering Identified Applications into ISF Tools Database

The LAPOC ensures that the site compares the required applications against the Application Catalog found in the ISF Tools Database. Any identified/surveyed applications found in the Application Catalog in the ISF Tools Database will be selected by the Command/Site for inclusion into the Command's/Site's Rationalized List. Surveyed applications not found in the Application Catalog of the ISF Tools Database must first be entered into the Catalog by the FAM or by the CDA or with approval of the FAM. Once entered into the Application Catalog, the application can be selected for addition to the Rationalized List by the Command/Site's Echelon II LAPOC Workflow Manager.

4.2.3.2 Selecting the Certified/Approved Application Version

When the LAPOC is adding the required applications into the Command's/Site's Rationalized List in ISF Tools Database, one of the initial steps is to search the Application Catalog by application long name, acronym or version. While in the Catalog, a check should be made for an approved/certified version of the application being added. LAPOCs should make every effort to utilize the approved/certified version found in the Catalog. Selecting the approved/certified version will accelerate and streamline the process of application rationalization, collection, submission, and certification. The preferred approved/certified version is always the CDA version. The CDA version is usually the latest and only approved version of the application. This process is known as certification by association (CBA).

The following steps, as explained in the ISF Tools User's Guide, will identify an approved/certified version of an application. In the Application Catalog:

- Look for "Approved" in the column labeled FAM Status.
- Look for an identified UIC in the POR/CDA POC column.
- Click on the number in the Usage column for an application record.
- In the pop up window, scroll down to the entry highlighted in blue.
- There should be an entry labeled "CDA RFS" in the RFS Type column and the RFS number should be followed by "-CDA" in the RFS # column. (For example, the CDA version for application ACMEAPP would show as "12345-CDA".)
-

For the CDA RFS entry, the column marked Certification Status should display the status as Certified

4.2.3.3 Creating a Rationalized List in ISF Tools

The list that identifies which applications commands desire to have transitioned into NMCI is known as a Rationalized List. Creating a Rationalized List is essentially a three-step process consisting of: 1) adding applications from the Application Catalog to the command's Rationalized List, 2) creating a Command Level RFS for each application, and 3) linking the application to each Implementation Group, where the application will be tested and deployed.

A command starts by adding each desired application from the Application Catalog to its Rationalized List A commands Rationalized List is identified by the Commands UIC / Name. There are two types of rationalized lists: Centralized and Command. A Centralized Rationalized List is managed by an Echelon II and will include all or some of its subordinate commands. Otherwise, a command will have it's own rationalized list that it manages itself, referred to as Command Rationalized List.

Once the correct UIC is determined, commands can add applications to a Rationalized List from either the Application Catalog view or the Rationalized List view. It is crucial to correctly identify applications by long name, acronyms, and versions. Application records with unknown version numbers will result in automatic NADTF disapproval. Again, if a desired application is not found in the Catalog, LAPOCs must contact their Workflow Manager, or the CDA/POR of the application to have it added to the Catalog.

4.2.4 Create User List and Begin Application Mapping

The process of associating applications to users or to client machines is known as application mapping. Application mapping commences, in NET, as soon as the Legacy Applications Transition process begins. It is highly recommended that sites collect application mapping information as they are performing the early steps of identifying and collecting Legacy Application data. Application mapping information will assist in application rationalization by identifying user demand.

This transition step is critically important to ensure that applications are mapped to users or to their desktops.

Failure to perform this step adequately and early in the transition process will result in users not having access to their needed applications at the time of seat rollout.

The Initial Application Mapping must be completed during the Identification Process. The Initial Application Mapping will be used as a reference when reconciling the Initial Rationalized List at Cutover -180.

Application Mapping is continually refined during the Rationalization and Collection Processes. The Final Application Mapping, which is due at Cutover –120, will be given to the EDS SM for delivery to EDS Transition Team for use in building User Profiles in the Active Directory. Those applications for which a user is not mapped will be removed from the Rationalized List.

It is understood that Commands/Sites will experience changes to their Final application mapping after the Cutover -120 deliverable. It is expected that some changes will occur as personnel change billets, transfer, etc. EDS requires that application mapping be locked at Cutover-30. This ensures that final changes are made to the User Profiles and the Active Directory, and Cutover is not jeopardized. After this date, changes to the application mapping will be handled at the discretion of the EDS Transition personnel. EDS has no requirement to address these late changes until Cutover completion.

NOTE: NMCI presently requires "application to seat" mapping. For further detail refer to Section 4.2.4.1.

4.2.4.1 NMCI Enterprise Tools (NET)

Application Mapping is accomplished using the NMCI Enterprise Tool, or what was formerly known as the NMCI Ordering Interface System (NOIS). NET automates the application mapping process by tying users listed for seat orders to the applications identified in the ISF Tools Database.

The NET is DON's single point-of-entry system for the Integrated Order to Delivery (IOD) process, which captures seat level detail needed by EDS for effective delivery and provides entry to the Global Addressing Library (GAL). The DON mandate for the use of NET is captured in Naval Message Appendix D14 for general information about NET, please refer to the NET website located at https://128.11.63.205/net/default.aspx.

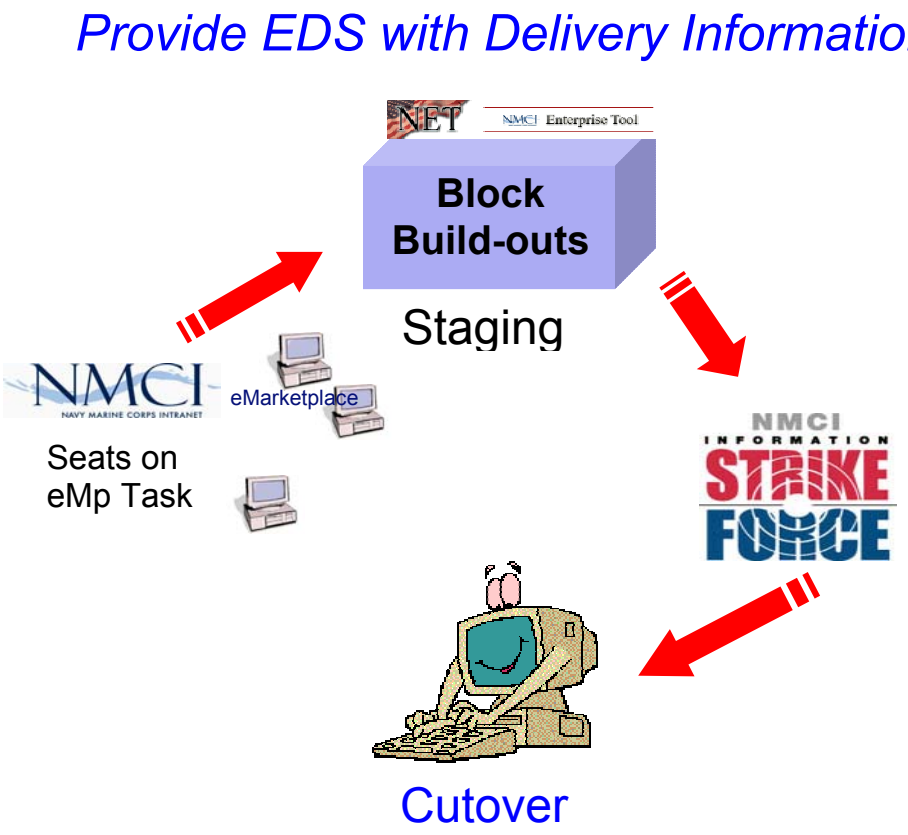


Figure 4-4. Example of IOD Process

NET interfaces with EDS for data consistency by providing: (See Figure 4-4 above.)

- ISF Tools for Legacy Applications data & site locations.
- eMarketplace (eMP) for seat ordering.
- Staging for seat deployment.
- Customizable roles and responsibilities within the Claimants.

- Workflow to move seats through the Claimants approval process.
- Ability for user profile transfer and communication between Commands.
- Links to Un-priced CLIN tool (Future Release).
- Enhances reporting capability.

Below are various modules available through NET.

- User Profile Module
  - User Profile Module contains all the information necessary to locate an individual at a site for delivery. Sample information includes: Name, phone number, email address, location (down to the cubicle level), organization, etc. User Profile Module includes the ability to reassign UICs within and across claimants.

- Existing Inventory Module
  - Optional module allows users to enter current inventory and inventory tracking number for association to a user profile.
  - This module tracks hardware only; it does not have the ability to track current application data.

- Seat Configuration Module
  - Creates seats by individuals or in groups.
  - Defines service dates for seat and options.
  - Creates and track shared accounts by individuals or groups.
  - Indicates seat delivery locations.
  - Performs edits, transfers, deletions and restorations.
  - Maps legacy applications and peripherals by individuals or groups.

- Seat Orders Module
  - Prepares Seats for order.
  - Routes Seats through approval chain.
  - Places Seats on order.
  - Push/Pull Seat order with eMp.
  - Creates build-outs and push to staging.
  - Performs global date changes.
  - Copies current Seat information to create new FY order.

- Reports Module
  - eMp Orders
  - User-to-CLIN Mapping
  - Seat-to-Applications Mapping
  - Shared Seats
  - CLIN Summary Reports (by status)
  - Buildout
  - Gold Disk Only
  - Legacy Peripherals
  - User Profile
  - Demand Model
  - MOD Deltas
  - NMCI Claimant Status
  - Ad Hoc

- Administration Module
  - Lookup table management
    - Claimant level
    - UIC-by-exception level
  - User role capabilities
    - Customized for each individual
  - Seat delivery locations automatically updated to eMp
  - Workflow management

- Import Module
  - Facilitates Claimant data conversion.
  - Uses MS Excel spreadsheets to move data into NET.
  - Includes the capability to incorporate/reconcile eMp data.

- Training Module
  - Virtual Classroom
    - Online tutorial
    - Online reference manual
    - Provides comprehensive package for practical, applied self-training.

Planned future enhancements modules will include: Embedded Only Help Module, Move/Add/Change Module, Demand Model, Account Management and Unpriced CLIN Tool Integration. To obtain training or inquire about NET please contact your appropriate NET lead (https://128.11.63.205/NET/Documents/Stakeholders/NET_Leads_21_July_03.xls). Training sessions are currently being held each month for claimants; information can be found at https://128.11.63.205/net/default.aspx.

Should NET be unavailable, or if the claimant has NMCI data in an electronic format, those customers may have their data imported before they start using the NET system. Since Claimants will be in different stages of their NMCI transition, the import files have been broken into 5 logical parts:

1. Delivery Location file,
2. Look Up file,
3. User Profile file,
4. Current (Seat) Configuration files (Legacy Apps and Peripherals), and
5. Seat Orders file. The NET Web site has complete descriptive examples on how to use an Excel document to import data. This information can be accessed at https://128.11.63.205/NET/Documents/General/Imports/Import.doc.

FY04 Seat Order Guidance

A Naval Message was released by the Director NMCI's Office regarding seat orders for FY04. Two important points to take from the Naval Message are as follows:

1. All NMCI orders and funding documents must be provided to assigned ACOs no later than 1 Sept 2003.

2. All orders must be placed into the NMCI Enterprise Tool (NET). NET is the enhanced seat-ordering tool that has replaced NOIS effective 21 Jul 2003. All activities shall use NET to

generate FY04 order requests and subsequent modifications. ACOs will not approve orders placed directly into eMP. All orders must be processed through NET.

4.2.5 Creating Application Loadsets and Role-based Profiles

To streamline the deployment of applications and to standardize usage of applications, applications on a Command/Site's Rationalized List can be grouped two different ways. Both Loadsets and Standardized role-based Profiles can be created using the Application Template feature found in ISF Tools on the Rationalized List view.

Loadsets and role-based profiles are standardized groupings of Legacy Applications built around organizations, seats and users. Common groupings of applications that are to be deployed to either all or a group of NMCI seats are known as Loadsets. Loadsets can be assigned to groups of seats according to organization or location.

Applications that are grouped according to user roles, e.g., admin or finance, are known as role-based Profiles and can be assigned to groups of users based on user roles and attributes. These groupings can be developed during Application Mapping and will expedite deployment of applications to the desktop, while maintaining flexibility for each Command/Site to ensure that the users have the applications they need. Further, profiles assist in the Command/Site's management of its software and applications.

Legacy Application Profiles are built around roles, which are the specific applications necessary for a user to perform his or her job. Profiles are the end result of mapping the applications to the user. They represent the groupings of applications that will be placed on each user's machine. These applications range from general Windows applications to the unique Legacy Applications specific to the user's billet or position. If Application Mapping is completed properly, profiles will be relatively easy to complete. Each user will have a list of the Legacy Applications they need. These roles will be combined with the Loadsets to create the user's profile.

Application Templates automatically appear at the top of the Rationalized List. They can be updated by clicking on the template name link.

When mapping applications, an Application Template automatically maps the applications contained within. Simply map the name of the template to seats or to users in NET.

A Loadset is based on creating a standardized grouping of applications around particular sub-sets or organizations of the DON. Common applications used by everyone in a sub-set, discovered during AM, will be incorporated into a Loadset. Loadsets consist of Enterprise Licensed Applications appropriate for all NMCI seats in this sub-set. A sub-set could be anything from the Navy or Marine Corps overall, down to a base, station, or site. For example, in the same manner in which the Gold Disk is for all NMCI users, a Blue Disk could be for the Navy, a Green Disk for the Marine Corps, a Purple Disk for Joint Applications, and a Silver Disk for Allied Applications, etc. Loadsets can continue further down to any component of the Navy or Marine Corps, or any component of a command/base/station/site, such as departments, divisions, wings, squadrons, battalions, units, etc. Loadsets can be designed to contain the Loadsets of subordinate organizations.

Loadsets are used to make up much of a user's profile. Any applications for a user not included in the Loadsets will be added into the profile. For example, a Navy Administrator's profile could consist of the Gold Disk, the Blue Disk, Loadsets for the organization the Administrator is in, and then any other applications the Administrator needs to do his or her job that are not included in the Loadsets.

Grouping applications is accomplished by simply clicking on the 'Create Application Template' button in the ISF Tool. In the popup window that appears, a name can be assigned to the template and applications can be assigned by selecting applications from the list in the right-hand column and clicking on the 'arrow' button to place them in the left-hand column. Applications can be added and removed from the template by toggling between the left and right columns using the arrow buttons. When finished, click on the 'submit' button.

Commands/Sites are encouraged to design Loadsets and Profiles as much as possible to streamline the application testing and deployment process. Lessons learned from previous sites have indicated that Loadsets and profiles are the key to successful Cutover.

4.2.6 Implementation Groups (IG)

ISF Tools uses Implementation Groups (IG) to identify the geographic locations where applications are to be LADRA tested. These locations usually coincide with a site where a Command is located and use the same site name and Physical Site Identifier (PSI) convention. In some cases an IG may be defined for every location if applications are to be tested at every location. In some cases IGs may be defined for sites chosen to be regional testing sites on behalf of a command

Site names and PSIs are used to identify locations where NMCI assets are deployed. The LADRA testing location may not always be the same as the deployment location. IGs are named using the same site name and PSI taxonomy as sites.

4.2.7 Linking Applications to Implementation Groups (IG) in ISF Tools

The final step in creating a Rationalized List is to link applications to their respective Implementation Groups (IG). An IG refers to the site where applications will be tested. It is the name given to the workbook used to record LADRA test results and DAA report data. An IG name consists of the official EDS site name and schedule increment.

Site and IG names are defined and maintained by EDS and held in ISF Tools. A list of the official Site and IG names are accessible from the log in page to ISF Tools. An additional view with search capabilities is accessible from the DS function tab in ISF Tools. It is important to note that site names are based on actual military installations, e.g., naval bases, naval air stations, air force bases, army posts, etc. They may also be based on leased commercial spaces or buildings that contain a command or activity, e.g., Crystal Gateway 4, Crystal Park 3, etc. Sites and IGs are not based on city and state. Each IG name is assigned a unique four-character identification code. These codes and IG names are used throughout NMCI for a variety of purposes, including naming network topography, i.e., seat and server farm names; specifying delivery locations for seat and CLIN orders in NET and eMarketplace; and in the enterprise seat rollout schedule. Increments are used in the enterprise seat rollout schedule to define groups of commands and seats to be rolled out at a site during a specified period.

An example of an Implementation Group is the following: applications to be tested and deployed at the site Washington Navy Yard in the 40K seat plan schedule increment would be linked to the Implementation Group name Washington Navy Yard – Increment 40k.

To link applications to Implementation Groups; first go to the desired Rationalized List view. Then click on the desired Implementation Group in the 'Impl Group' pull-down menu at the top of the Rationalized List page. The EAGLE Data Management Team assigns the choices available in the 'Impl Group' pull-down menu.

4.2.8 Gather In-Use Peripherals and Drivers

A peripheral is any device that is connected to or works in conjunction with a workstation/desktop. Peripherals can be external devices such as a mouse or keyboard, or they can be internal devices, such as CD-RW drives.

Legacy peripherals are those peripherals not turned over to the EDS as part of AOR. There are legacy desktop peripherals, which are connected to a single NMCI seat and sit on a desktop, and there are legacy network peripherals that are standalone units connected directly to NMCI and multiple NMCI users share them.

Legacy Peripherals are:

- Printers, scanners, plotters, chart-makers, Personal Digital Assistants, digital cameras, zip drives, etc.
- Connected externally to the NMCI seat.
- Not shared with any other NMCI seat.
- Windows 2000 compatible.
- Cannot impact Service Level Agreement (SLA) performance.
- Cannot violate NMCI security policies.

Drivers are the associated software designed to allow the peripheral to function with the workstation/desktop. They may be defined as:

- Software that interfaces with a computer to a specific peripheral.
- A device driver is the associated software designed to allow a peripheral to function with the workstation/desktop. There is device drivers for printers, displays, CD-ROM readers, diskette drives, and so on. A device driver essentially converts the more general input/output instructions of the operating system to messages that the device type can understand.

NOTE: Peripherals and their drivers are not part of ISF Tools Database nor included on the Legacy Applications Rationalized List. They are not ***applications***. ISF doesn't certify drivers or peripherals, only applications.

4.2.8.1 Peripheral Support Software

Sometimes there is software associated with peripherals to support the hardware. This supporting software is not a driver, but an application associated to support the peripheral. For example, a chartmaker may have support software that enables the user to make charts (i.e., Enterprise Systems Chartmaker will have the Enterprise Systems Chartmaker Design program with the actual chartmaker). This software should be listed on the Rationalized List and submitted for certification and testing as an application

4.2.8.2 Bundled Peripheral Support Software

Sometimes, the peripheral driver and peripheral support software are combined into one complete package in support of the peripheral. This is referred to as bundled software. In this case, the bundled software is listed on the rationalized list and submitted for certification and testing as an application using a single RFS. The contents of the bundle should be listed in the Additional / Special Instructions section of the RFS, as well as the legacy peripheral for which this RFS is intended.

4.2.8.3 Peripheral Categories

There are two categories of peripherals: (1) customer/user owned and (2) NMCI contract provided. For those peripherals ordered and provided by the NMCI contract, the devices, drivers, and their maintenance are included with the peripheral order and provided by EDS. Legacy Peripherals are those devices that are provided by the customer/user. Procurement and maintenance of Legacy Peripherals and their associated software/drivers are the responsibility of the customer/user. However, EDS maintains an extensive library of peripheral drivers and may be able to provide the appropriate driver. EDS will not require drivers if they are easily downloaded from a website or already included in the Windows 2000 Operating System. The site should be prepared to deliver drivers if required. Non-driver software that is associated with a peripheral is considered a Legacy Application and is to be handled as such in accordance with this guide. Legacy Peripheral installation is a customer/user responsibility, while connectivity and driver installation are the responsibility of the ISF.

When considering peripherals in the development of an application, please consult the Microsoft Compatibility list. As long as the peripheral has a Windows 2000 compatible driver (either from Microsoft or from its own manufacturer) and it doesn't violate any IA rules or SLAs, it should be able to transition into NMCI. To see the Windows 2000 compatible list from Microsoft, go to:
http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/

4.2.8.4 Peripheral Transition

EDS will attempt to transition the device provided the installation is “plug and play”. “Plug and play” refers to the ability of Windows 2000 being able to use its own driver for the device, or a Windows 2000 compatible driver is available from the Microsoft Windows 2000 website. Additional efforts beyond “plug and play” are still covered in the contract and may take additional time. The customers/users are expected to provide drivers for their peripherals.

Windows 2000 capability will be determined by the legacy desktop peripheral appearing on the list of compatible hardware devices as shown on the Windows 2000 Check Hardware and Software website:

http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/default.asp

Windows 2000 includes approximately 7,500 drivers. Other drivers may be listed on the Microsoft Windows 2000 compatibility web site that may be available for the peripheral. Drivers provided by the customer/user should be Windows 2000 compatible. If the driver is not found in the Windows 2000 Operating System, cannot be downloaded from the Microsoft Windows 2000 compatibility web site, a Microsoft compatible driver is not provided by the customer/user, and is not part of a designated legacy application; EDS will be unable to transition the peripheral.

At this point the customer must obtain a compatible driver or reengineer the existing driver. If reengineering the driver is the solution, the customer may have EDS reengineer the driver using CLIN 29 or have some other source provide the reengineering.

If a compatible driver is not obtainable and the existing driver cannot be reengineered, the peripheral will not transition to NMCI. At this point, the customer/user may replace the peripheral via CLIN 23 or other sources.

When the new NMCI seat is ready to be deployed, the legacy desktop peripheral will be attached and the Windows 2000 driver will be loaded (if needed). The legacy desktop peripheral will be tested to verify it is working properly.

Legacy Peripherals will not be provided with maintenance or support. As the legacy devices reach end-of-life, replacement devices must be purchased off of CLIN 23.

4.2.8.5 Rationalized Peripheral and Driver List

The site must provide the ISF with a list of their Legacy Peripherals and their associated drivers. This is necessary to ensure the ISF will provide connection for the peripherals and, since the desktop is locked down, provide installation for the associated driver. The Site Representation of Legacy Peripherals is a list in a spreadsheet format. The template is provided in Appendix G1. The list of peripherals and their associated drivers are turned over to the ISF SM. The list of these components is not part of the Legacy Applications Rationalized List in the ISF Tools Database. The Site delivery of the Peripherals and Drivers Rationalized List to the ISF SM starts the internal ISF evaluation and rationalization of these items.

4.2.9 Identify Legacy Application Servers

4.2.9.1 Legacy Server

Legacy Servers are those systems that include existing customer software and hardware currently in use at a site by people performing the mission or business of the DON that are not included in the NMCI standard services or the CLIN catalog. Legacy servers may be individual servers hosting one or more applications or systems consisting of multiple servers, console/workstations, supporting devices/systems and possibly network devices. Current legacy servers may run any of several possible operating systems (including, but not limited to, Windows 2000, Windows NT 4.0, Solaris, HP-Unix, Mac OS, Novell) and may host server as well as client applications and agents.

4.2.9.2 Identifying Legacy Servers

The site must identify their Legacy Servers to the EDS to ensure that the EDS Transition personnel can properly map the desktop to server connection. This list is usually generated using a spreadsheet and delivered to the EDS SM. A template example of this deliverable can be found in Appendix G7.

4.2.9.3 Server Only Operating Systems, Applications and Tools

Non-Windows 2000 Legacy Application Server operating systems (for example: Solaris, HP-Unix, Novell, Linux, Windows NT, Mac OS, etc.) will not be included on the Legacy Applications Rationalized List nor tested in NMCI. For migration into NMCI, servers with non-Windows 2000 operating systems will need to interface with the NMCI Windows 2000 backbone.

Server tools that will be loaded to NMCI desktops need to be listed on the Legacy Applications Rationalized List and submitted for NMCI testing. Sun Net Manager, HP Openview, TNG Unicenter, and Peregrine IND are examples of server tools that have administration clients that can control servers externally from a desktop. The client end of these tools will be identified and submitted for NMCI testing. Such server tools can be left alone on the server and, in that configuration, will not require NMCI testing.

NOTE: Some of these tools have the option to use agents; however, agents are not authorized for use in NMCI per the NMCI Application Ruleset.

4.2.10 Identify Reachback and Datashare

In order for EDS to properly map and route users and their machines to servers, files, databases, etc., the site must identify all reachback and datashares requirements. NMCI will replace all existing Legacy

network operating system and electronic mail servers. However, legacy applications, files, datashares, databases, servers, etc. will still exist and must be mapped to the new NMCI desktops. Therefore, for a successful transition, specific reachback requirements must be identified to EDS to ensure they will be included in the transition.

Appendix G6 provides a template for use in identifying datashare and reachback requirements. Other network methods such as *tracert* and *traceroute* can be used to identify network connections and their associated IP Addresses. However, you should consult with your network manager prior to use.

4.2.10.1 Reachback

Whether working in NMCI or the Legacy environment, users need constant access to a vast array of network drives, peripherals, databases, data stores, networks and services to accomplish their jobs. In the Legacy environment these service connections were simplified, over time becoming a generic consequence of the way of doing business. However, with the migration to NMCI, many of them will not initially transition with the user, so some provisioning or Reachback will be required to link them through the Boundary 2 (B2) into the Legacy BAN or through the Boundary 1 (B1) to other legacy assets. The concept of Reachback as it relates to NMCI is that users must identify all paths, connections and interfaces employed in mapping their NMCI seat back to other legacy drives, databases, servers and networks. Systems Administrators will be able to properly map/reroute those services through the B1 and B2 until such time as the optional services themselves can be migrated into the NMCI enclave. To ensure that users have uninterrupted access to the services and resources they need, it is vital that the LAPOC properly identify and document all service paths and connections associated with each seat during the Identification phase of the Rapid Certification process.

4.2.10.2 Datashare

Datashares act as repositories and central access points for a continuously evolving number of datasets. This arrangement ensures greater reliability and flexibility while increasing overall accuracy and maintainability. The datashare may represent the actual data resource residing in a shared file, optional drive, shared drives, database, server, library, network, or legacy environment.

For NMCI, users need constant access to their datashares, especially during transition, when the datashares will exist in the legacy environment. Access to these assets must be guaranteed to ensure that continuity of business practices. The LAPOC must ensure that all datashares are identified, documented and submitted to EDS. EDS must ensure the new NMCI seat is properly mapped to the datashares. This may include reaching across the NMCI boundaries (1 & 2).

4.2.11 Late Identification

Customers must identify their Legacy Applications on time. Per CNO Naval message of 30 September 2002 (301245Z SEP 02), all applications were to be identified and entered into ISF Tools Database by 29 November 2002. Legacy Applications identified after this time are considered "late." Lateness jeopardizes their inclusion in seat Cutover. However, if the application is identified before the specific site Cutover date it is still considered Legacy and will be transitioned by EDS per the contract.

Applications identified after the start of Cutover are considered "emergent." Emergent applications are not considered to be Legacy Applications based on the NMCI contract terms. The Command/Site and/or the Echelon II Command will be responsible for the financial implications associated with NMCI Certification and transition of emergent applications. Please refer to Appendix C for further details of the Late Application Identification and Submission Process.

4.3 RATIONALIZATION

Figure 4-5 depicts the Rationalization process. The goal in Rationalization is selecting only those desktop and server-based applications, both COTS and GOTS, required to support command or DON missions, goals, and business processes.

After the Legacy Applications have been identified, the information is carefully examined, scrutinized, and analyzed by the Command/Site for rationalization. Rationalization consists of categorizing the applications by type and functionality, and then applying NMCI policies, rules and Navy/Echelon II/local standards to eliminate those that violate the rules and standards. The customer is encouraged to eliminate any unnecessary, redundant, or nonstandard applications that are not absolutely required to support the site's mission, processes, and goals.

General Notes on Rationalization

Rationalization of Legacy Applications is not dependent on completing the Identification steps. Rationalization can occur concurrently with the Identification steps. Customer decisions on the disposition of applications (e.g., eliminate, consolidate) can occur as soon as sufficient information becomes available. Additionally, rationalization may (and ideally should) be independent of the NMCI transition process. However, NMCI transition provides an excellent opportunity to achieve the objectives of the rationalization process.

Echelon II Commands must help determine which applications should be retained in service. Echelon II Commands are expected to review all subordinate Command's/Site's Rationalized Lists for approval. They must formally approve the Final Rationalized List in the ISF Tools Database by indicating those accepted applications as rationalized. A Command's/Site's Rationalized List will not be accepted until it has been reviewed and approved by the Echelon II Command.

The end state of this effort is the submission of the Final Rationalized Legacy Application List via the ISF Tools Database. Any additions to the Rationalized Legacy Application List after 29 November 2002 will require NADTF approval.

Navy Message R 301245Z SEP 02 CNO Washington DC Enterprise Strategy for Managing NMCI Applications and Databases directs action to achieve common operational picture of the Navy's applications and databases in DADMS and the continued use of the ISF Tools Database as the primary tool for ordering and implementing applications in NMCI. This message:

- Directs all Echelon II Commands to ensure that their Final Rationalized List of all NMCI applications is reflected in the ISF Tools Database within sixty (60) days of the date time group of this message (29 Nov 2002).
- Requires the approval of the applicable FAM and Navy IO for the subsequent addition of applications to ISF Tools Database by Echelon II Commands and subordinate Commands.
- Mandates that every Navy application will have a designated CDA and/or owner identified by name with contact information.
- Specifies a process to be followed to track all Quarantined applications.

NOTE: If no owner for an application is identified, the application will not be allowed to migrate to NMCI and any reference to it will be removed from ISF Tools.

As part of the rationalization process, the following actions need to be accomplished:

- Derive raw application list from the ISF Tool database.
- Categorize applications by type and functionality.
- Apply NMCI Rulesets.
- GOTS and COTS Rationalization.
- Apply available standards.
- Apply Application Mapping.

4.3.1 Standardization and the Gold Disk

In order to reduce the number of applications within the enterprise, the DON has begun implementing standardization of applications. Since there are numerous applications that can perform the same function, the DON has begun selecting standard applications to be used across the enterprise. In this manner, applications that perform the same function are minimized to provide for a smaller list of Legacy Applications.

The first major step in standardization is the NMCI Standard Seat Service or Gold Disk (Appendix B). The DON has determined that all NMCI desktops are to employ the applications contained in the Gold Disk. Further, per CNO Washington DC (N09T) message dated 120155Z JUN 02, the DON requires all Echelon II Commands to eliminate any unnecessarily duplicative application(s) from their Rationalized List. If an Echelon II Commander requires an additional version of an application on the Gold Disk or other applications performing the same function, the Commander must request an exception from the Naval IO and the applicable FAM as outlined in the aforementioned message.

NOTE: The unique function being performed by the unique application, and why it is operationally required, needs to be included.

Similar to the Gold Disk, the DON has deemed certain Legacy Applications as standards. The latest list of standards can be found in the CNO Washington DC (N09T) message dated 120155Z JUN 02 (Appendix D). Each Echelon II Command is required to establish application version control following the Standardized COTs and GOTs applications list. Echelon II Commands need to update application versions on their Rationalized List in the ISF Tools Database to reflect the versions listed in this message.

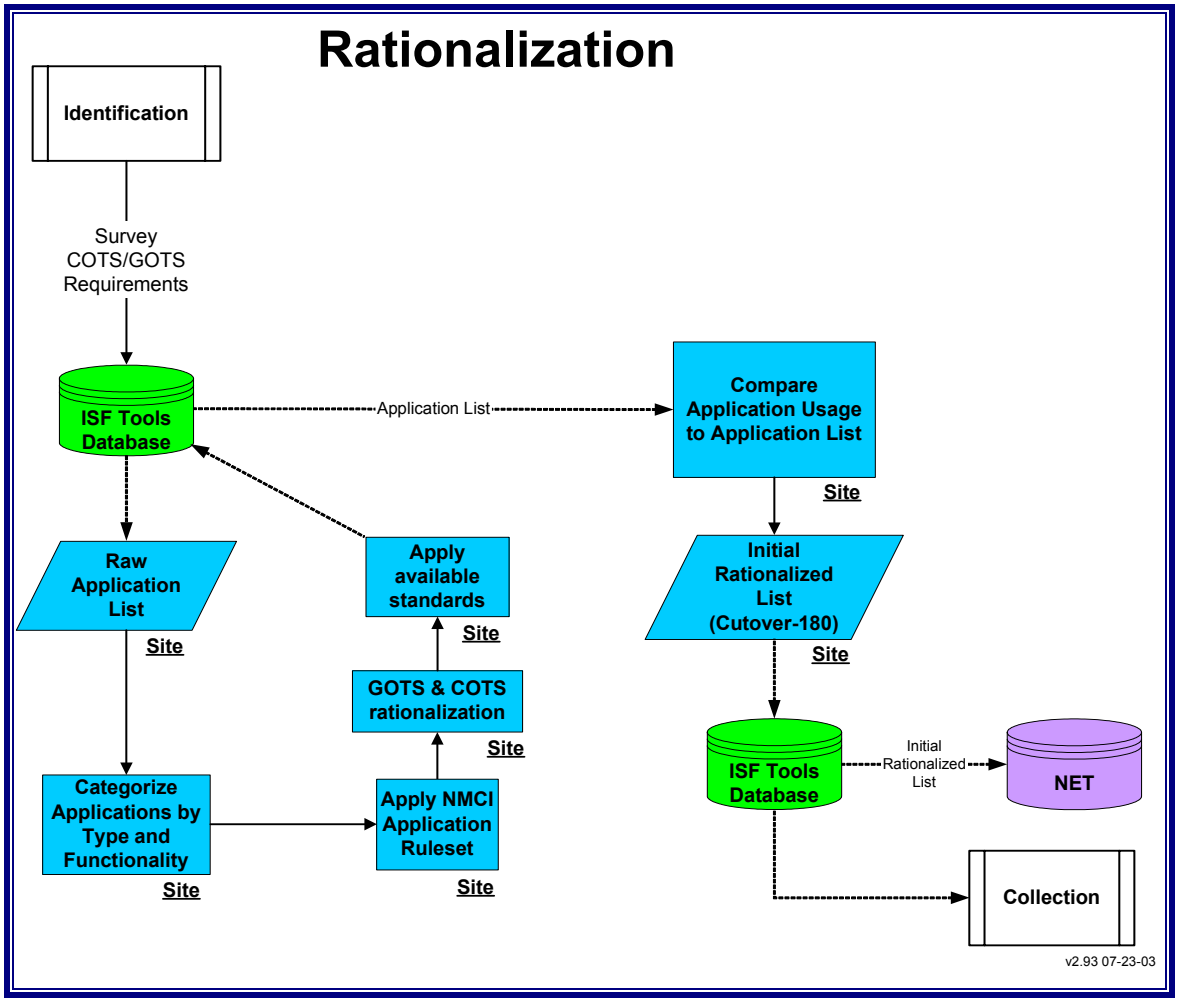


Figure 4-5. Rationalization

4.3.2 Derive Application List From the ISF Tool Database

Once the site has entered all Legacy Apps into the ISF Tools Database, a list of applications for that site can be created. This list and other information will be used in the Rationalization process.

4.3.3 Categorize Applications by Type and Functionality

Legacy Applications should be grouped and categorized by type and functionality. Grouping and categorizing is a useful tool in determining which applications are mission essential. For example, all of the graphics and design applications can be grouped into a category called “Graphics Design”. When all of these graphics and design applications are grouped they can be reviewed for overlap, redundancy, excess, and relevance. From this the Command/Site selects their rationalize applications.

4.3.4 Determine if Application is for Software Development

During this step, the Command/Site will determine if the application is used in the development of software applications. Software development tools can include functions such as database creation and administration, code generation, compling and any other application for software development. This step

is necessary because software development tools cannot be used on standard NMCI seats. Software development tools can only be used on NMCI Science and Technology Seats (S&T).

If the application is determined not to be a development tool, then other standards and rules will be applied to the application as part of the rationalization process.

4.3.4.1 Simple vs. Complex Developer Applications

Once the application has been categorized to be a development tool, then it must be determined whether it is a simple or complex application.

A simple application is defined as a standalone application that requires installation on an NMCI workstation only, and has minimal to no dependency on network connectivity to function. The requirement for these applications to use the network for file share and printer access does not make them complex. For example, most word processing applications are considered simple applications.

Applications that require network connectivity for standard operation are, for the purposes of this program, defined as complex applications. Any applications that have a separate front end and back end, and require network connectivity to be fully functional, are considered complex. Server based and client/server applications are examples of complex applications. See the Section 4.3.4.2 below on this type of NMCI Seat.

If the software development application is categorized as simple it will be removed from the ISF Tools Database List and will undergo no further tracking/testing by EDS. If the software development application is categorized as complex EDS will require evaluation and testing to determine the application's impact on the network. Thus, it must be tracked in the ISF Tools Database and appear on the Command's/Site's Legacy Application Rationalize List.

4.3.4.2 Science and Technology (S&T) and Developer Seats

S&T or Developer Seats are designed for use by application developers, science and technology researchers, and anyone for whom a "locked-down" desktop will prohibit mission accomplishment. It is not intended for these seats to be purchased as work-arounds to the NMCI implemented desktop lockdown. These desktops can be requested under CLIN 38. Due to the likelihood of systems failures, EDS provides minimal support to S&T seats users. Customers who order these seats are responsible for maintaining desktop operation and functionality. EDS will assist the S&T seat user if the seat needs to be re-imaged due to operating system failure or if the Gold Disk applications need to be reinstalled. EDS retains responsibility for non-developmental application support. Further, EDS remains responsible for hardware support. Developer application support is available through CLIN 23 for S&T seat use only.

4.3.4.3 Apply NMCI Rulesets

All applications will be reviewed against the NMCI Ruleset for compliance. Applications that are found not in compliance with the Ruleset are subject to NAVY IO waiver or are Killed and removed from NMCI. Not all Rulesets are waiverable and not all Ruleset violations result in a Kill. More detailed explanation of the Ruleset requirements can be found in Appendix E.

Request for waivers for applications that violate these rules will be submitted by the responsible Echelon II command to the Navy IO. FAM will adjudicate all waiver requests for the FAM's Waiver Process referenced in Section 4.3.4.3.1 below.

The following rules apply to GOTS and COTS applications within NMCI:

1. Windows 2000 (W2K) Compatible
2. NMCI Group Policy Object (GPO) Compatible
3. No Duplication of Gold Disk Software or Services
4. Comply with DON/NMCI Boundary 1 and 2 Policies
5. No Setup, Installation, Uninstallation, Update and Auto Update Tools or Utilities
6. No Games
7. No Freeware or Shareware
8. No Beta/Test Software (Authorized on S&T Seats Only)
9. No Application Development Software (Authorized for S&T Seats Only)
10. No Agent Software.
11. Gold Disk Compatible
12. No Peripherals, Peripheral Drivers or Internal Hardware
13. No personal, non-mission, or non-business related software
14. No 8/16-Bit Applications

Other applicable rules may emerge from the DON or the Echelon II command.

In addition to the above rules, CDAs are encouraged to consider development requirements specific to supporting IT-21, the Marine Corps Tactical Network (MCTN), BLII and the TFW. The goal is to standardize applications and databases across all networks, if feasible.

4.3.4.3.1 FAM Waiver Process

Applications that fail an NMCI Ruleset during the Release Deployment Process and that are waiverable will require the CDA to complete a DADMS Waiver questionnaire. The questionnaire must be completed within 5 duty days as stipulated in the FAM Mid-Term Application and Database Rationalization Process v7.7 document dated 05/15/03 available at https://www.dadms.navy.mil/. The FAM will review the questionnaire and make final determination on the waiver request. Waiver requests that are disapproved result in the application being removed from the Rationalized List. Applications with an approved waiver are allowed to complete the Legacy Transition Process.

Navy Message R 252230Z JUL 03 CNO WASHINGTON provides action to ECH II Commands to FAM approved applications.

- For Commands commencing NMCI cutover after 1 October 2003, limit authorized application to those designated as FAM "Approved" or " Allowed with restrictions."
- Should application on the disapproved list be considered mission critical, submit recommendation and justification for proposed work around by 8 August 2003 to Director, Navy Staff (DNS).
- "By 15 August 2003, appoint a migration manager to lead the migration strategy and implementation plan."
- "By 1 October 2003, eliminate dual desktops retained solely to support disapproved application."

- Exceptions to this policy must be requested, with Echelon II concurrence, from the appropriate FAM or DNS.

For amplification see Naval Message (Appendix D25.)

Further guidance is offered below and referenced in Naval Message Appendix D24.

- After 1 October 2003 FAM disapproved applications will no longer be loaded onto NMCI and they will not be approved for retention on any legacy seat.
- Disapproved applications mapped to users or seats in NET will be automatically filtered out before the seat build out to staging process begins.
- Only FAM "Approved" or "Allowed with Restrictions" applications that technically cannot operate on NMCI (Fail LADRA/AIT Testing) are authorized to remain on quarantine seats and legacy networks.
- All FAM disapproved applications on the NETWARCOM Most Wanted and high priority application listing that so not receive FAM approval will be removed from the work list.
- If all reasonable efforts to obtain FAM approval have been exhausted via the waiver process and the Command/Site feels that an appeal of the FAM decision is warranted, submit that appeal to OPNAV CIO at OPNAVCIO@navy.mil. (Naval Message Appendix D25.)

4.3.4.4 GOTS and COTS Rationalization

The site will analyze the list of Legacy Applications for redundancy, functional overlap, and multiple versions of the same applications that are being used at the site. Duplicate and redundant applications will be eliminated prior to compiling the Rationalized List.

NOTE: If no owner for an application is identified, the application will not be allowed to migrate to NMCI and any reference to it will be removed from ISF Tools.

4.3.4.5 Apply Available Standards

Many Echelon II Commands/Sites have their own established software standards. If there are specific or other DON/DoD standards, they will be applied to the application list for processing.

4.3.4.6 Websites and URLs

Websites, especially those that download an application or portion of an application to the desktop, need to be identified and tested by EDS. These websites must be included in the Rationalized List; otherwise, if not tested and approved, access to these websites cannot be guaranteed. The long-range plan for NMCI is to test, approve, and list in the ISF Tools Database the websites that customers have requested. Then sites will be able to select from a common list of websites that have been tested. If there is doubt whether a website falls into this category, place it on the Rationalized List and work with EDS to verify it during testing.

4.3.4.7 Adding an Application to the Legacy Applications Rationalized List

An application must first reside in the ISF Tools Database. If selected from the Application Catalog, it will appear on the Rationalized List. All Legacy Applications that reside in the in ISF Tools must receive approval from the appropriate FAM before they can be deployed into NMCI. Once an application has

been added to the Rationalized List, the Command should submit a Command Level RFS to request certification of the application for deployment to NMCI.

Legacy Applications that are not contained in the ISF Tools Application Catalog require FAM approval before entry into the ISF Tools Application Catalog.

4.4 COLLECTION

The Collection process is a Government responsibility. Figure 4-6 depicts the important elements of this step.

After the Rationalized List is created using the ISF Tools Database, the Legacy Applications and supporting documentation must be collected for submission to EDS Site Manager.

There are certain steps and procedures that need to be taken within the Collection process. These processes are listed below:

- Associate to a Certified Application
- Identify Licenses
- Identify Desktop and Server connectivity (Network Diagram)
- Perform Final User/Application/Machine/Server/Peripheral Mapping
- Finalize Site Loadsets
- Generate and Gather IA Documentation and Items

4.4.1 Request for Service (RFS)

A RFS is an EDS document used by the transitioning activity to identify a legacy application requirement and collect necessary information for application packaging, certification and LADRA testing. All applications to be used at the transitioning activity in NMCI will require a RFS submission. The RFS should be treated as a work order to EDS to perform a service.

4.4.1.1 Creating a Request for Service (RFS) in ISF Tools

There are two kinds of RFSs: 1) CDA RFS, 2) Command Level RFS.

4.4.1.1.1 CDA RFS

The CDA, vendor, or program manager of an application will create a CDA RFS (Request For Service) for that application. A CDA RFS identifies a request for an application that is developed and supported by the CDA to be certified and approved for use within NMCI. Once an application is certified and approved in NMCI, it is then accessible for selection and use by any command. The application with a certified and approved CDA RFS is the preferred application record to use when making additions to the Rationalized List. The Command should research the ISF Tools Application Catalog for an existing application record with a certified and approved CDA RFS. If a CDA RFS does not exist for the requested application, either the application does not have a CDA or the CDA has not been properly identified. Only the CDA of the application can submit a CDA RFS.

The existence of a CDA RFS is easily determined when looking up an application in the Application Catalog. In the Application Catalog view, across from the application record name, is a POR/CDA POC link that displays POC information for a CDA. By clicking on the Usage link found alongside the

POR/CDA POC column and then clicking on the CDA RFS link that appears in the popup window highlighted in blue, a view of the CDA RFS form will be displayed.

When a CDA RFS is submitted, the following items need to be collected to meet the media submission requirements:

- Installation Instructions and Test Scripts/Plans (See Appendix G for examples)
- Media and License Validation
- Network Diagram (desktop-to-server connectivity)

Further details regarding CDA RFS submissions can be found in the NMCI Release Development and Deployment Guide (NRDDG) (published separately).

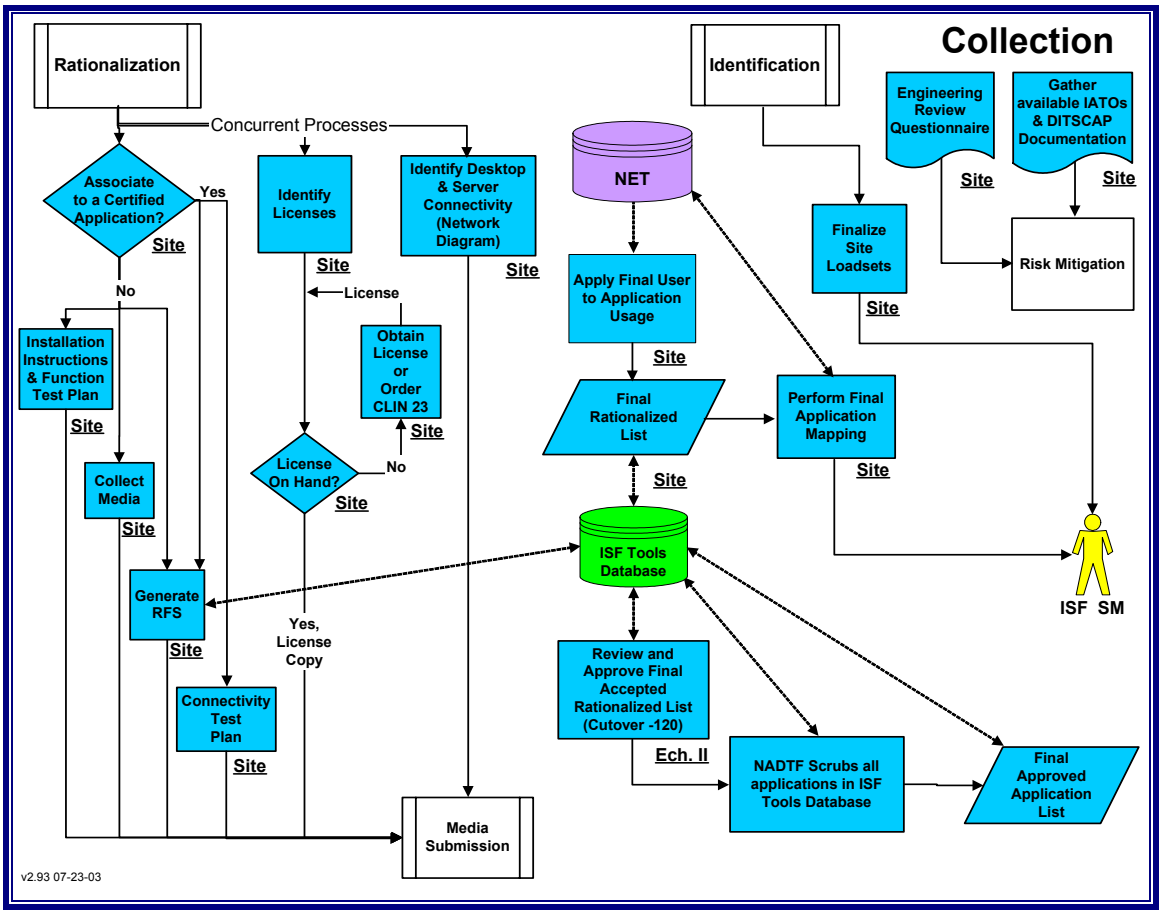


Figure 4-6. Collection

4.4.1.2 Command Level RFS and Rationalized List

A Command Level RFS is a request by the transitioning activity to use a specific application in NMCI. All applications to be used at that activity require a Command Level RFS submission. The RFS is accessed and submitted electronically through the ISF Tools DB.

Commands can exist at multiple geographic locations. Commands can have subordinate activities that exist at different geographic locations. Some locations may consist of one Command and others may consist of multiple Commands. Sites are names (Site Definitions). Site names are maintained by EDS and can be found in the login page of ISF Tools under the link Site/PSI List (excel format). And found in ISF Tools under the DS tab. Each site has exactly one-PSI code. The term PSI is equivalent to Site Code or 4-Code, which is maintained by EDS. Site names and PSIs are used to identify locations where NMCI assets are deployed.

A site is a permanent geographic location where one or more operating units carry out their mission. It is a geographic, not organizational, unit. A site is a military station, base or complex, training complex, or commercial complex. In general, a site can be either an actual military base or one that is military base-like. Only one site can reside per base.

ISF Tools uses Implementation Groups (IG) to identify the geographic locations where applications are to be LADRA tested. The LADRA testing location may not always be the same as the deployment location.

These IG LADRA testing locations can usually coincide with a site where a Command is located and use the same site name and PSI convention. In some cases, an IG may be defined for every location if applications are to be tested at every location. In some cases, IGs may be defined for sites chosen to be regional testing sites on behalf of a Command.

Commands creating Rationalized Lists in ISF Tools may opt to create a Centralized Rationalized List, at the Echelon II or III level, for example. One instance for generating a Centralized Rationalized List is to allow a Command that exists in multiple geographic locations to utilize a single Rationalized List. Another instance for generating a Centralized Rationalized List is to allow multiple subordinate activities existing under the same Command to utilize a single Rationalized List. In either instance, a Command Level RFS should be submitted for each application contained within the Rationalized List.

Once a Rationalized List is created, applications are then linked to each respective IG where the applications are to be tested. The IGs utilized by a Command Rationalized List UIC can be found in the "IMPL" pull-down field at the top of the Rationalized List page in ISF Tools. The EAGLE Data Management Team maintains these available lists of IGs. If the IG list is not complete or requires changes, contact the EAGLE DMT for assistance.

Currently however, a Command Level RFS is required. A Command Level RFS, is created by clicking on the 'Create RFS' links found on the right-hand side of the Rationalized List page across from the Application Name. The RFS form appears in a popup window displaying the necessary data fields to be populated. When finished, click on the 'submit RFS' button and an RFS number is automatically assigned. If changes are required, the RFS can be updated by clicking on the RFS number link. The RFS will receive an initial status of 'RFS Submitted'. An RFS can be updated only while it is in 'RFS Submitted' status. Once the AIT lab begins work on an application and the RFS reviews a new status, the RFS for that application can no longer be updated by the command.

In the future, when a CDA RFS already exists, a command will not be required to submit its own Command Level RFS. A command will automatically inherit the CDA's RFS number when adding an application to its Rationalized List.

4.4.2 Identify Licenses

Commands/Sites must comply with all legal copyright rules regulations and laws. Government Agencies may require proof of compliancy with copyright laws at any time. However, for transition purposes, EDS does not require verification of compliancy with copyright laws. EDS does require proof of licensing for the copy of the application that is being submitted for NMCI Certification Testing. If a license is not available, proof must be obtained through an approved vendor, government agent or ordered through CLIN 23.

4.4.3 Identify Desktop and Server Connectivity (Network Diagram)

It is the responsibility of the Command/Site to provide a Network Diagram to EDS Site Manager The Network Diagram should show desktop and server connectivity, as illustrated in the example. (Appendix G5.)

4.4.4 Perform Final Application Mapping

The Command/Site performs the final application mapping in NET, tying the users listed for seat orders with the applications identified in the ISF Tools Database. The Final AM is then turned over to EDS Site Manager using the software Report function from NET. In the near term, there will be an automatic interface so that the mapping data can be submitted automatically. This step should be completed 120 days before cutover. The Final application mapping should be used in the verification of the Final Rationalized List. It is understood that the application mapping will change between the time of submission and cutover. The Command/Site can continually update application mapping in NET up until the time of the OCM run. Once an OCM run is completed, all application mapping is locked until after cutover, which changes can be made via the MAC order.

4.4.4.1 Create the Final Rationalized List

The Command/Site will perform a final review of the applications entered in the ISF Tools Database Application List. -Application mapping is applied against this list for verification of the Rationalized List. Once the final review is complete, the Final Rationalized List is forwarded to the appropriate Echelon II Command for review and approval.

4.4.4.2 Review and Approve Final Accepted Rationalized List

The Echelon II Command reviews and approves the Final Rationalized List. This approval is required for the list to be formally accepted. This review and approval produces the Final Accepted Rationalized List.

4.4.4.3 NADTF Scrubs Final Accepted Rationalized List

NADTF personnel will scrub the Final Accepted Rationalized List.

- Apply the NMCI Ruleset.
- Check the existing DON Standard Applications List.
- Check if the application is already certified and performing the same function.

- Check to ensure the version number of the application is the latest available.
- Verify the Command/Site's Unit Identification Code (UIC).
- Verify that a CDA is assigned (if applicable) along with a previously submitted CDA RFS.

The NADTF will kill applications not passing the criteria. Once finished, NADTF will approve the Command's/Site's Final Accepted Rationalized List, producing the Final Accepted Applications List.

4.4.5 Engineering Review Questionnaire (ERQ)

The ERQ is a document designed to collect all information pertaining to an application. The ERQ is used to analyze a system's requirements and configuration. This information is critical to the post-transition Accreditation procedures for the development of DITSCAP documentation and the Systems Security Authorization Agreement (SSAA). The ERQ is a prerequisite to begin the Risk Mitigation Phase. If the ERQ has not been completed or updated, the System Analysis Team and the Site Representative, CDA, and POR/PM must complete the ST-ERQ in lieu of the ERQ. While not required during the Rapid Certification Phase, the ERQ information is most readily available as part of the Collection process of the Rapid Certification Phase. The ERQ template can be found at www.nmci-isf.com.

4.4.6 Gather Available IATOs and DITSCAP Documentation

If any prior Interim Authority to Operate (IATO) or DoD Information Technology Security Certification and Accreditation Process (DITSCAP) information exists for a legacy application being submitted, it should be collected and stored for use in the Risk Mitigation Phase. If this information does not exist, the application owner will need to fulfill this requirement before the application can be fully accredited in the Risk Mitigation Phase.

4.5 MEDIA SUBMISSION

Figure 4-7 depicts the steps for Media Submission. This process is primarily a Government responsibility, but there are several aspects of the process that are joint or EDS-only responsibilities. Refer to the NMCI Legacy Applications Submission Guide found on the NMCI web page at www.nmci-isf.com/downloads/NMCILegacyAppSubmitGuide.doc The NMCI Legacy Applications Submission Guide details the procedures and documents needed for submission of media and documentation to EDS.

After an application's media and support materials are collected, it must be submitted to EDS to begin the NMCI Certification process. As mentioned in the Collection process descriptions (Section 4.4) there are two types of submissions: Legacy Applications submitted through the CBA process and new Legacy Applications.

All Legacy Application media and materials will be submitted to the EDS SM. If the EDS SM has not arrived on site, the Command will hold all materials until the SM arrives.

4.5.1 Initial Assessment and Testing Decision

The Command/Site will turn the submission over to the EDS SM. EDS will perform an Initial Assessment of the submission, which includes a Completeness Review and a determine where the application will be processed for certification.

If the submission passes the completeness review, the Legacy Application type is determined:

- CBA Legacy Applications (with their RFS) will be examined and retained on-site for processing.
- New Applications (non-CBA applications) will be reviewed to determine the Certification process. EDS will decide to either:
  - Retain it on-site for Local Deployment.
  - Send it to the San Diego AIT Lab for Packaging and Certification.
- Copies of all network diagrams and other documentation will be retained by EDS.

NOTE: Certification process and location is an EDS decision.

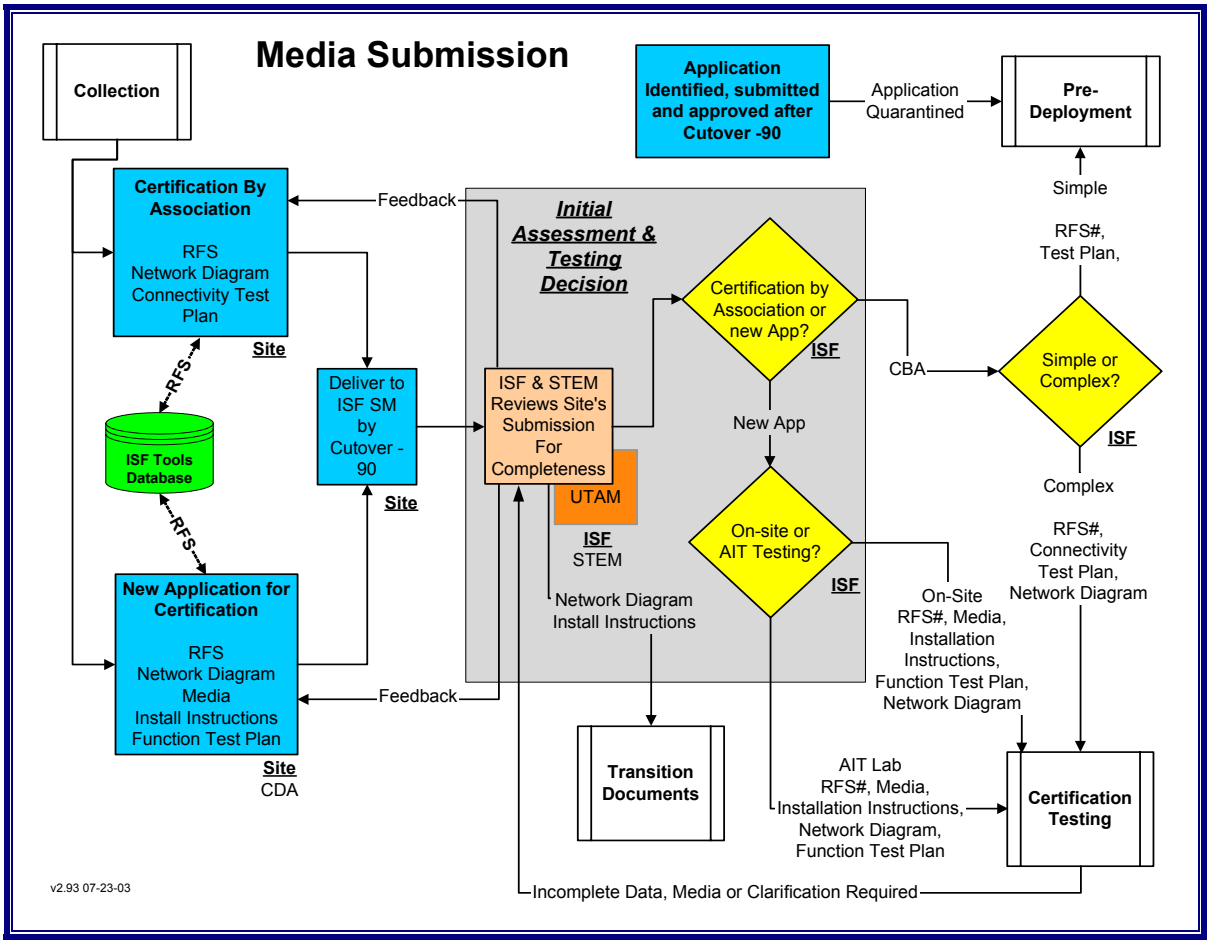


Figure 4-7. Media Submission

4.5.2 Submission Deadlines

All application submissions are due to the EDS SM by Cutover -90 days. Customers must submit their media and supporting documentation on time. Missing this deadline will cause those applications to be late, and subsequently to be subject to the Late Identification and Submission Process. (See Appendix C) EDS must have time to process (Certify) the application for transition.

If the media and supporting documentation are not submitted by Cutover, the application will be considered an "emergent" requirement and not a Legacy Application based on the NMCI contract terms. The Command/Site and/or the Echelon II Command/Site will be responsible for any financial implications associated with the NMCI Certification and transition of these applications.

4.6 TESTING

Testing consists of two processes, AIT Lab Testing and On Site Testing as depicted in Figure 4-8. Lab Packaging, Certification and Testing are done only at the AIT Labs in San Diego. On-site Packaging and Testing are done via the PIAB and LDSD&T tests on-site. Applications are never certified on-site. The Testing processes are discussed below.

During the testing process the application status is recorded and tracked in the ISF Tools Database. AIT Lab personnel and SSE teams will record the status of the various steps within the process using this tool.

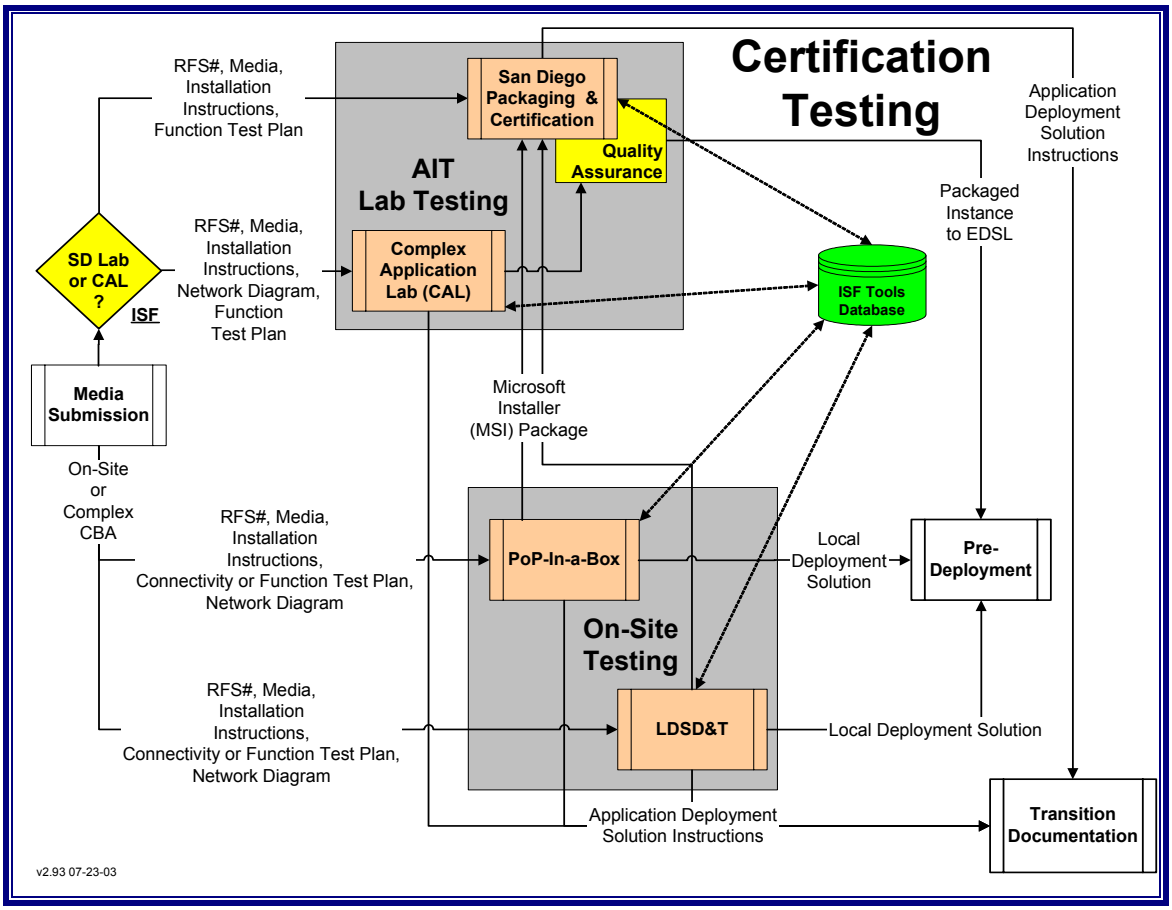


Figure 4-8. Certification Testing

4.6.1 Local Deployment vs. Push

Several criteria are used to determine how an application is handled and processed. User base and Enterprise impact are major criteria used to determine the process an application will go through. Applications that have an overall Enterprise appearance and a high user base are likely to be processed through the San Diego AIT Lab to create a packaged Enterprise solution that can be centrally managed. Large Enterprise (CDA) applications are prime candidates for central packaging and push. Those applications with a low user base and local impact only are good candidates for the On-Site Testing Processes and to be Local Deployed. The Application Mapping is one of the main tools used to determine an application's user base.

NOTE: EDS has the responsibility to determine the most effective way to deploy a Legacy Application, and they will route the Legacy Application to the appropriate testing location and method.

A Local Deployed application is one that does not utilize the packaging and push processes. Local Deployed applications are placed on the NMCI desktop through means other than the Novadigm Radia push (explained below). There are many ways the application can be loaded to the desktop; examples include manual hand load, central server load, File Transfer Protocol (FTP) download, etc.

NOTE: EDS will determine the most efficient process to Local Deploy an application**.**

When an application has an enterprise exposure and a high user base, locally deploying that application is not practical. Therefore, creating a centrally managed enterprise solution is usually the best option. An application is "pushed" through an automated process that originates at the San Diego AIT Lab and runs through a set of software servers from the NOC through the server farm to the site. This "push" process is accomplished, managed, and distributed using the Novadigm Radia tool and active directory. In order for an application to be automatically delivered (pushed) to the desktop, the application must be packaged for delivery. Applications that are packaged and pushed using Novadigm Radia take advantage of centralized software management that delivers applications to the desktop without the user going through an "install" process.

4.6.2 San Diego Packaging & Certification

Figure 4-9 depicts the process of San Diego Packaging & Certification. EDS site personnel will send the applications to the San Diego Certification lab (AIT Lab). CDAs should submit their versions directly to the San Diego AIT Lab after making the appropriate entries in the ISF Tools DB and creating a CDA RFS.

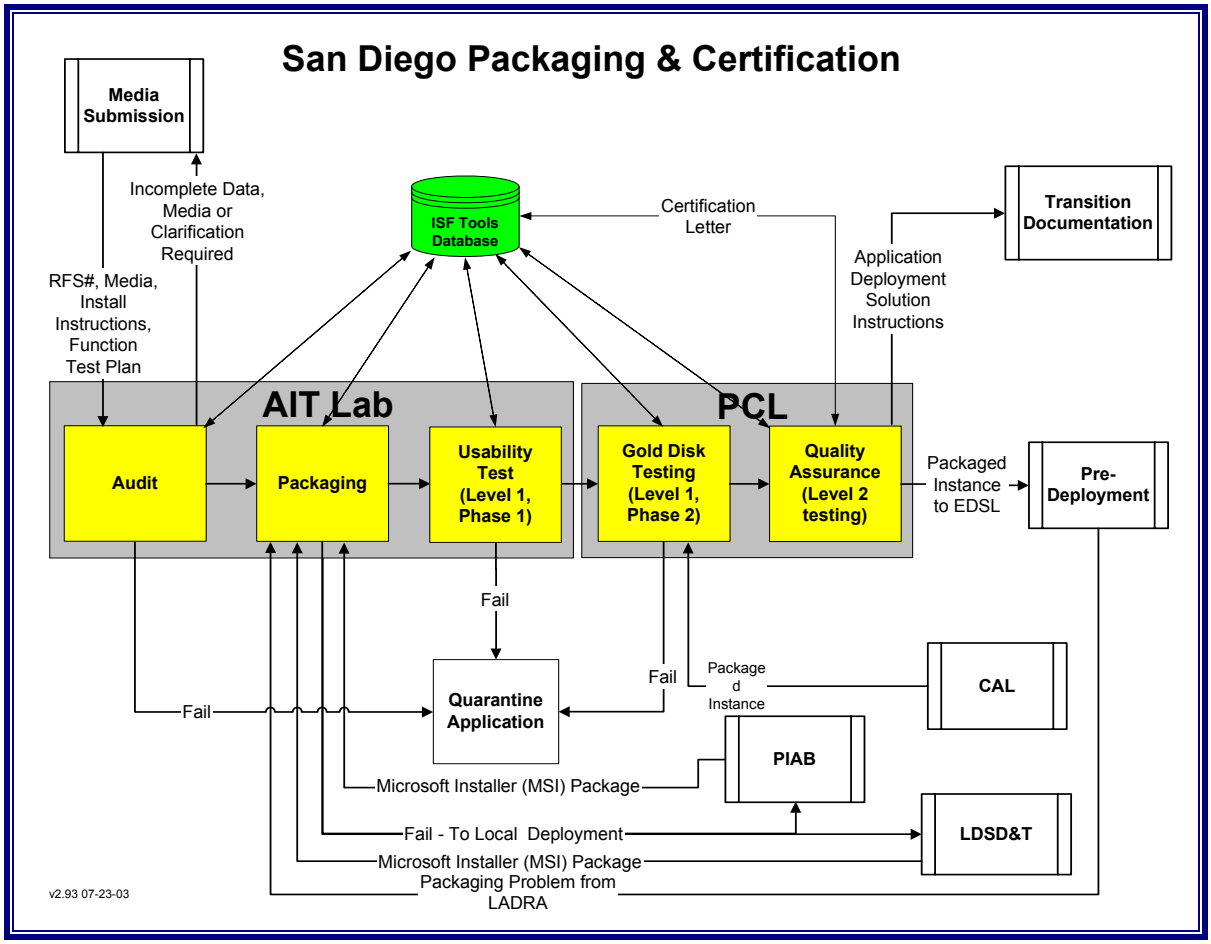


Figure 4-9. San Diego Packaging and Certification

Once received in the lab, applications are processed through Packaging Audit by EDS lab personnel to verify that the media packet is complete and there are no viruses. Any installation instructions are reviewed for completeness, along with all other needed documents and information.

The AIT or EAGLE Team personnel notify the Command/Site/CDA of problems with any submissions. The ISF Tools Database is updated by AIT Personnel to track the status of the application during testing, certification and packaging.

After a successful audit, the application is packaged using Novadigm Radia, then goes through the Lab Usability Test (Level 1 Phase 1). If the application fails to package, the application will be returned to the Command/Site for Local Deployment processing or the CDA for remediation. If the application successfully packages, it is then run through the Lab Usability Test.

The Lab Usability Test determines if the "Package" executes successfully and the application runs properly in the Windows 2000 environment. It does not test end-to-end connectivity, run a trace, nor involve "users". Failure of the Usability Test will send an application to Quarantine. Next, the GPO Ruleset in the Enterprise GPO established by the Navy and EDS is applied. An application's failure to operate with the Enterprise GPO will cause that application to fail and be quarantined.

Upon completing the Lab Usability Testing, the application enters the Proving Center Lab (PCL) and is tested against the Gold Disk of standard NMCI applications for interoperability issues. Failure of the Gold Disk Test will send an application to Quarantine.

Any configuration notes recorded as part of the packaging and testing process are stored as transition documentation.

When an application has completed the Certification Process at the San Diego AIT Lab and NMCI Certification has been granted, the NMCI Certification Letter is created in the ISF Tools Database. A copy of the Certified Radia Instance is stored at the Enterprise Definitive Software Library (EDSL).

Some applications will require on-site testing to make sure that they function properly for the site. These applications will undergo a Usability Test on site or in the CAL.

For those Legacy Applications that are to be CBA to an already NMCI Certified application, many of the early steps in the process are skipped, including the Radia packaging. The Radia instance of an application that is already in existence is used for this CBA situation. These applications are already packaged, so they can immediately proceed to the on-site Usability Test sub-process as detailed in Section 4.6.5 of this guide.

If an application fails during the Packaging portion of the process, it will be referred back to the site for processing as a Local Deployment application. A package can fail the Packaging process if the media is not valid, installation instructions are incomplete or other issues are found with the packaging.

NOTE: During the Packaging and Certification process, the status of the various steps is recorded and tracked in the ISF Tools Database by AIT Lab personnel.

4.6.3 Complex Application Lab (CAL)

Figure 4-10 depicts the CAL process. The CAL is primarily a post transition tool for use by CDAs for introducing applications or changes into the NMCI environment. The primary function of the CAL is to test priority applications that need outside connectivity.

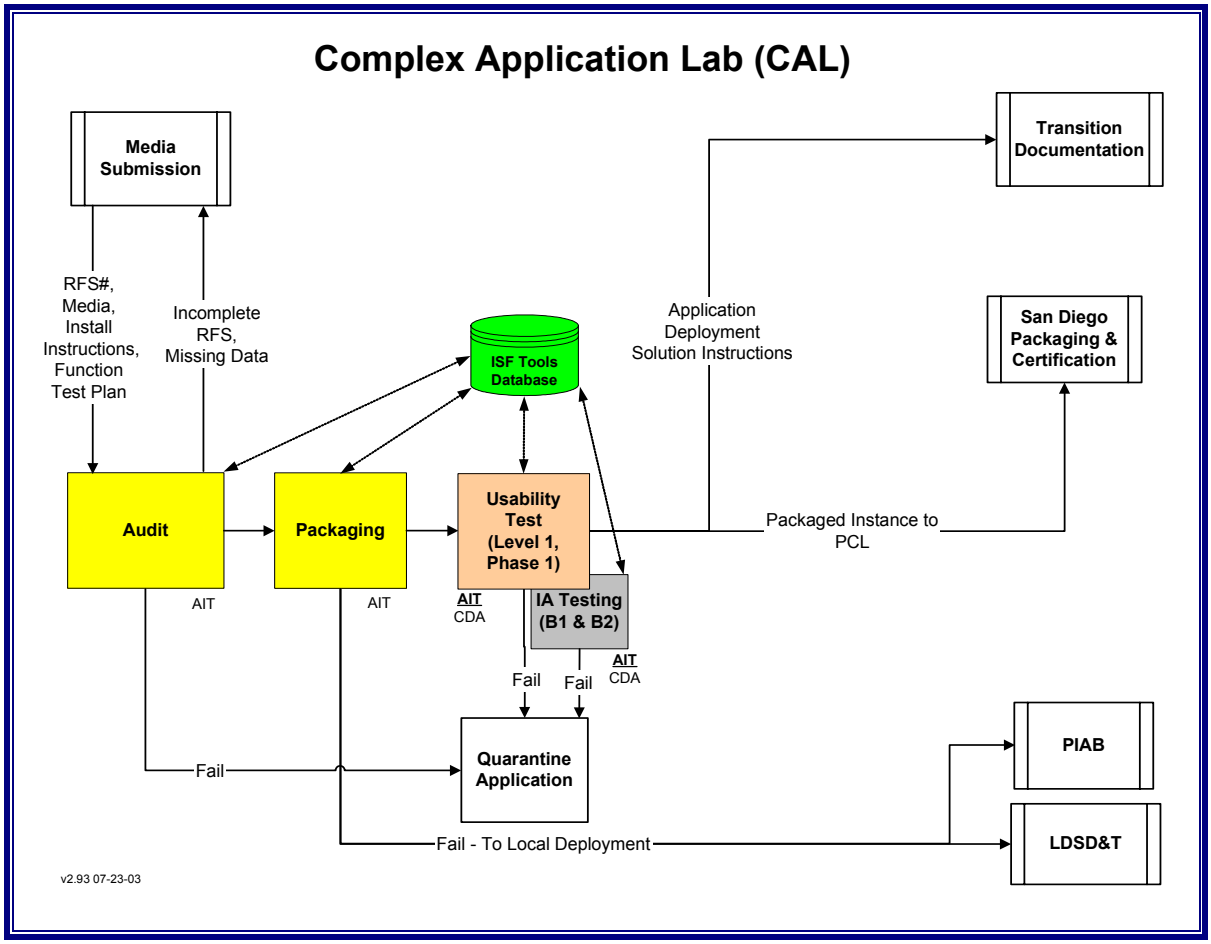


Figure 4-10. Complex Application Lab (CAL)

EDS can use the CAL to process transitioning legacy applications to determine solutions. Optionally, the CAL can be used as an overflow lab to the AIT Lab.

Those applications selected for the CAL are handled like any other application destined for the AIT Lab in San Diego. Once in the lab, EDS will determine if it is best to process the application through the CAL.

NOTE: It is EDS' decision to utilize the CAL to process the application. The Command/Site/CDA may provide input into this decision.

Once in the CAL, applications are run through a Packaging Audit by CAL personnel to verify that the media submitted is valid and there are no viruses. Any installation instructions and other needed documentation are reviewed for completeness. The Lab personnel notify the Command/Site/CDA of problems with any submissions. AIT personnel track the status of the application during testing, certification and packaging and update the ISF Tools Database.

Information Assurance (IA) testing is performed as part of the Audit and Usability testing. These steps test the application for compliance with the IA policies, rules, settings and infrastructure. Failure of IA testing will lead to the application being quarantined. The data captured during the IA testing is used during the Risk Mitigation Phase for Accreditation leading to the DITSCAP documentation and the SSAA.

If an application testing issue arises such as incomplete data or bad media, or if clarification is required, the Lab personnel will work with the EAGLE and/or the CDA to correct any issues so that testing can be completed in a timely manner. If during the Audit the application is found to be non-deployable within NMCI, the application will be quarantined. For the reasons why an application may fail Audit please see the NMCI Ruleset found in Appendix E.

Next, the applications are "packaged" into an electronically deployable "instance" using special software called Novadigm Radia. These "instances" allow the application to be centrally deployed and managed using Active Directory. If the application cannot be packaged or has failed the NMCI Ruleset, then the application will be sent for local deployment testing

Once successfully packaged, the application is run through the CAL Usability Test (called Level 1, Phase 1 and 2 Testing). The Lab Usability Test differs from the site Usability Test. Though both tests have common steps, the Lab Usability Test does not test end-to-end connectivity, run a trace, nor involve "users". Its primary purpose is to determine if the "Packaged Instance" of the application executes successfully and if the application runs properly in the Windows 2000 environment. Failure of the CAL Usability Test will cause an application to be quarantined.

As part of the Lab Usability Testing, the application is tested against the Gold Disk of standard NMCI applications for interoperability (Level 1 Phase 2 Testing). Failure to successfully interoperate with the NMCI Gold Disk will result in an application being quarantined.

Next, the packaged application instance proceeds to the San Diego AIT Lab for the Quality Assurance (Level 2) testing step. This is essentially a quality control check of the application's packaged instance. After successful completion of this final test, the packaged instance is sent to the EDSL for deployment to the network and seat.

NOTE: During the CAL processes, the status of the various steps is recorded and tracked in the ISF Tools Database by AIT personnel.

4.6.4 On-Site Testing

Applications retained on-site for Local Testing can be tested using one of two tools available to the EDS SSE Team: the PoP-In-A-Box (PIAB) or the NMCI Test Seat used in the Local Deployment Solution Development and Testing (LDSD&T) process.

To begin any On-Site Testing, the applications are evaluated for their suitability for packaging and push to the desktop. Applications selected for local packaging will be processed by the EDS SSE team via the PIAB (if there is a PIAB on site). If there is no PIAB at the site, the application cannot be packaged for push. If the application is unsuitable for packaging, it can be processed through the PIAB or LDSD&T for a Local Deployment solution.

4.6.5 PoP-In-A-Box (PIAB)

Applications start with an Audit by the EDS SSE team to verify that the media submitted is valid and there are no viruses. Any installation instructions are reviewed for completeness. Problems with any submissions are turned over to the STEM for resolution with the site. Figure 4-11 depicts the PIAB process.

The SSE Team then determines how they will deploy this application. Their choices are Package and Push or Local Deployment.

4.6.5.1 PIAB Package and Push

The application is "packaged" into an "MSI instance" using special software from Microsoft. Once the application has been successfully packaged, the application instance and all supporting documentation are sent to the San Diego AIT for further packaging in Novadigm Radia for push to the desktop. Once that Novadigm Radia package is returned to the PIAB, the instance is sent for local usability testing. Applications that fail to successfully package will be sent to Prepare Local Deployment Solution to be processed as local deployed applications.

4.6.5.2 PIAB Local Deployment

Local Deployment applications and all supporting documentation are sent for Local Usability Testing. Applications that fail Local Usability Testing will be quarantined. After the Usability Testing, the application is tested against the Gold Disk of standard NMCI applications to look for interoperability issues. Failure to interoperate with the Gold Disk will cause an application to be quarantined.

Applications that successfully pass all steps of the PIAB are ready for final Legacy Application Deployment Readiness Activity (LADRA) testing and deployment. Local Deployment applications are retained on-site for deployment. On-site packaged and tested applications are copied and sent to the San Diego AIT Lab ("Packaged Radia Instance" is another name for the packaged application) for the Final Certification Lab Process and load to the EDSL servers.

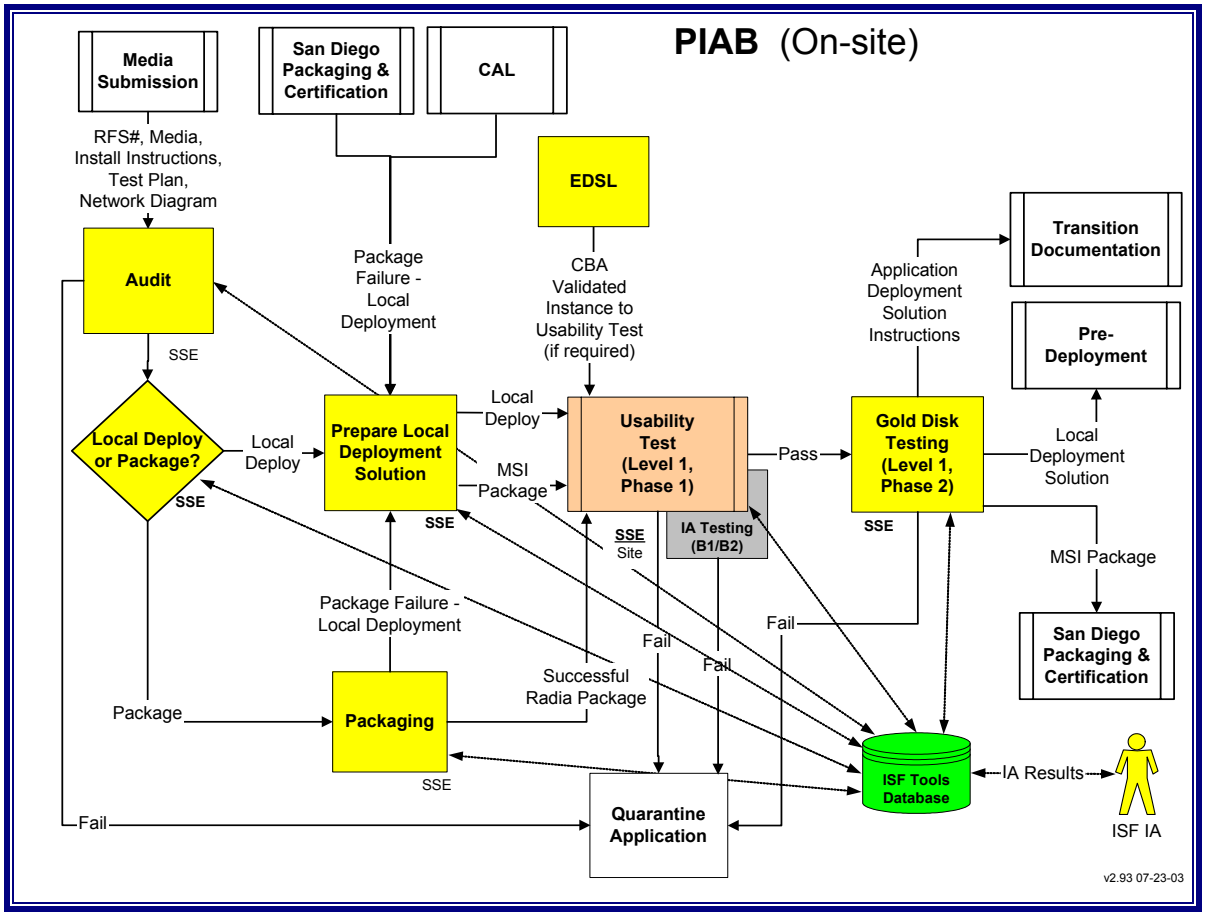


Figure 4-11. PoP-In-A-Box (PIAB)

NOTE: During the PIAB process, the testing and certification status is recorded and tracked in the ISF Tools Database by the SSE team.

4.6.6 Local Deployment Solution Development and Testing (LDSD&T)

The LDSD&T process is depicted on Figure 4-12.

LDSD&T is used when local testing is warranted and a PIAB is not available. LDSD&T requires the NMCI Base Infrastructure to be installed and active, but does not require connection to the live NIPRNET environment. EDS uses standard NMCI Seats installed on the Base Infrastructure to perform the application testing and processing. These standard NMCI Seats have special software installed and are called NMCI Test Seats.

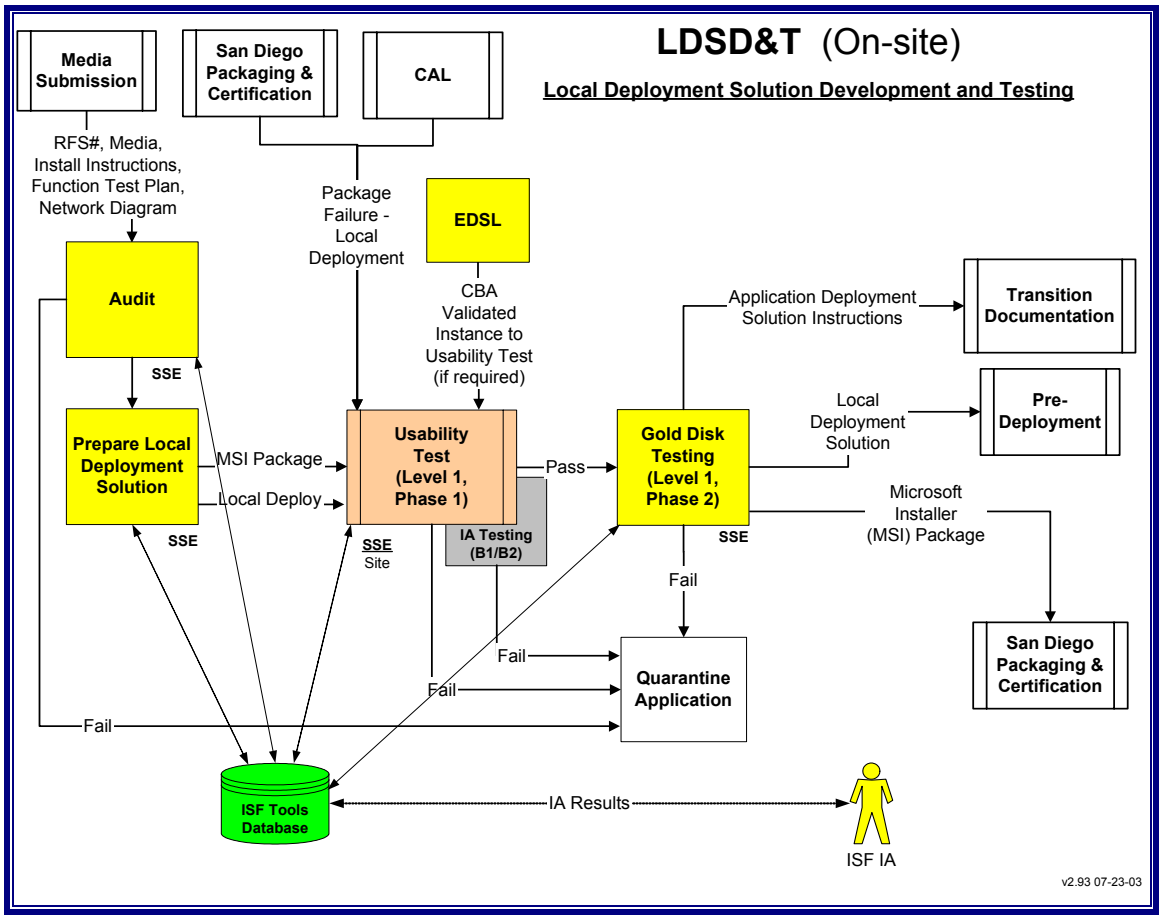


Figure 4-12. Local Deployment Solution Development and Testing

The LDSD&T process starts like all other testing processes with an Audit of the submission. Applications are Audited by the SSE team to verify that the media submitted is valid and there are no viruses. Any installation instructions are reviewed for completeness. Problems with any submissions are turned over to the Site Legacy Application POC for resolution with the site.

Applications are then sent to Usability Testing Applications that fail Local Usability Testing will be quarantined.

After the Usability Testing, the applications are tested against the Gold Disk of standard NMCI applications to look for interoperability issues. Failure to interoperate with the Gold Disk will cause applications to be quarantined.

All applications that are processed as part of LDSD&T will also proceed through the Legacy Application Deployment Readiness Activity (LADRA) testing (as described later in this guide). Often the SSE team will combine the LDSD&T and LADRA testing into one seamless procedure. Note: Though LDSD&T and LADRA may be combined into one seamless procedure, the separate and distinct steps of each must be performed and successfully completed. Thus, performing LADRA does not mean skipping the steps of LDSD&T. Failure to complete the LDSD&T steps will lead to the application failing to deploy.

NOTE: During the LDSD&T process, the status of the various testing steps is recorded and tracked in the ISF Tools Database by the SSE team.

4.7 USABILITY TEST

The Usability Test is a sub-process of the Certification and is used in the on-site testing processes. EDS has primary responsibility for this step, but the government can be involved in the joint process.

The Usability Test is conducted on-site with either PIAB or an LDSD&T. The PIAB test environment simulates the NMCI environment and allows a network trace to be performed when the application is active. The NMCI Test Seat is an actual NMCI production desktop with special configurations and software for testing the application and running traces. The PIAB is used when the NMCI base infrastructure is not complete. Once the base infrastructure is in place, NMCI Test Seats are utilized to complete application processing.

This sub-process starts using the following applications:

- Newly packaged on-site.
- On-site certified application that will be locally deployed.
- An already packaged NMCI Certified Radia Instance that has been sent to the site from the San Diego AIT Lab.

The packaged application is pushed to, or the local deployed application is deployed to, a “test cell” in the PIAB or NMCI Test Seat. For an application that will use CBA, EDS can gain access to this previously certified application by downloading it via the on-site FTP server. This application is then deployed to the test seats for processing.

If there are any special configuration changes needed to get the application to install properly, that configuration information is documented as an ADS Instruction. The Command/Site user/application owner/CDA will assist with any configuration changes.

After the application has been configured, actual users are brought to the PIAB/NMCI Test Seat as part of Usability Testing. Commands/Sites are responsible for identifying and scheduling a designated user/tester. A designated user/tester should be familiar with the installation and usage of the application. The designated user/tester must come to the testing area ready to process the application from end-to-end when scheduled. To ensure proper support during application testing, Commands/Sites should designate a primary and alternate user/tester for every application.

NOTE: Commands/Sites are responsible for identifying and scheduling a designated user/tester.

If the designated user/tester is not available to test the application, that application cannot be tested. The STEM and EDS SSE team, in coordination with the Command/Site and SIL, will attempt to contact and schedule the user/tester twice. If, after two attempts, the user/tester cannot be scheduled or fails to support the application processing/testing, the application will be set-aside for Quarantine. Processing an application Quarantined for lack of user support will be done when EDS resources are available as long as it does not delay Cutover.

The user portion of Usability Testing is accomplished using a test script (if one has been provided) or free form by the user/tester. An example of a Test Script can be found at Appendix G4. In addition, while the testing is being done the SSE team will run the network trace (EtherPeek software) to trace the ports, protocols, and services used by the application. The results of the application test will be documented by the SSE Team and sent to EDS IA personnel. Each application is also reviewed for compliance with B1 and B2 firewall policies. For more information on NMCI IA and Boundary Definitions, the reader is referred to the NMCI Contract and Appendix H. The PIAB/NMCI Test Seat results (which include the network trace) and other information are used during the Risk Mitigation Phase.

The Packager/Certifier will analyze the configuration changes that were needed to allow the application to install and run properly. If needed, the application will be repackaged with the new configuration information. Any configuration changes that cannot be included in the packaged application are noted so that they can be performed as part of the desktop deployment. The repackaged application will be pushed to a test cell in the PIAB or NMCI Test Seat. It will be analyzed to verify that the repackaged application is working properly and no further configuration changes are needed.

As the final step, the Packager/Certifier will prepare the packaged application for the Gold Disk testing.

NOTE: If an application fails any part of the Usability Test (non-Win 2K compliant, poor interoperability, non-GPO compliance, non-B1/B2 compliance, etc.) it will be quarantined. After the initial seat Cutover, this application and its solution must be re-evaluated for a final disposition.

4.7.1 Transition Documentation

The Transition Documentation process is an EDS responsibility, but is described here for informational purposes.

Application information for a site is stored in the Site Folder (a collection of documents kept on-site for immediate and future reference), the Application Document Storage site (an electronic storage site used by EDS), and the ISF Tools Database.

These various information storage locations help EDS complete their job and assist in the creation of the Applications Deployment Solution Instructions. These documents detail the connectivity solution for each application at a specific site. This information will be used in the Risk Mitigation Phase of the site's NMCI transition.

4.7.2 Information Assurance (IA)

NMCI security and IA are critical to the success of NMCI. Through layers of technical protections and procedures, NMCI enables its users to access information and services with the trust necessary to do their jobs. Defense-in-depth protection mechanisms are deployed in a layered fashion forming boundaries at multiple levels within the security architecture. This process ensures resistance to attacks and minimizes

the possibility of a security breach due to a weakness (known or unknown) at any single security component. The defense-in-depth protection strategy provides security features to NMCI systems and data. These features are confidentiality, integrity, availability, accountability, and non-repudiation. Elements comprising various aspects of IA provide those security features.

IA consists of two parts: policy and implementation. Policy is a government responsibility, while implementation has been delegated to the ISF. The NMCI DAA sets the policy for the Enterprise B2 and the GPO, which has also been referred to as Boundary 4. The Enterprise B1 policy is known as the Navy Marine Corps Enclave Protection Policy (NMCEPP) and is set by OPNAV/CNO. For more information regarding boundaries, refer to Appendix H. ISF is responsible for the implementation of the Boundary and GPO policies set by the NMCI DAA and OPNAV/CNO. The implementation of the policies is accomplished in two phases, the Rapid Certification Phase and the Risk Mitigation Phase.

During the Rapid Certification Phase, the overall goal and end state is seat migration. This means the NMCI desktops are operational and can function in the NMCI environment. Before the seats can be migrated, the Enterprise B1, B2, and GPO policies are implemented. IA data is collected on the applications, but is not analyzed. This data will be used in the Risk Mitigation Phase. NMCI DAA has Authorized access to Legacy Applications using a type accredited Boundary 2. The NMCI DAA reviews the weekly report submitted by the ISF to ensure compliance.

IA Testing occurs during the Usability Test. PIAB and NMCI Test Seats are used to test the B1, B2, and GPO compliance. The application is loaded onto the NMCI test seat (either PIAB or LADRA). If the application is tested using a NMCI Test Seat and then functions properly, it is compliant with B1 and B2 firewall policies. If the application is tested using a PIAB, port and protocol data will be reviewed for compliance with the policies. All port and protocol data is passed on to the Risk Mitigation Phase. To test GPO compliance, the application is loaded on a test seat and if it functions properly, it is compliant with GPO. For more information on GPOs and examples of those that will be used in NMCI refer to Appendix H.

As mentioned in the Usability Testing section, any application that fails IA compliance testing will be quarantined. A team of ISF and IATT members will review the application and make recommendations for modification during the Risk Mitigation Phase. Once the proper modifications are made, the NMCI DAA will grant an IATO/Authority to Operate (ATO) and the application will be allowed to migrate to the NMCI environment. Packaged & Certified Applications will receive ATO automatically once the application is fully packaged. (THIS IS ONLY VALID FOR **SIMPLE** A PPLICATIONS and not complex applications.)

4.7.3 Enterprise B1, B2, and GPO Operational Management

Appendix H gives an overview of the IA Operational Management and NMCI Architecture. The appendix shows where B1 and B2 are implemented. Each boundary serves a purpose. The B1 (NOC) protects access to NIPRNet and Internet. The B2 performs similar functions as B1, except that the rules are more permissive for an interface with existing internal Navy and USMC networks.

4.7.4 Risk Mitigation

Risk Mitigation enforces the acceptable level of risk that the NMCI DAA will accept for transitioning a legacy system into NMCI. The reasons for performing Systems Transition are three-fold:

1. Reduce the number of quarantined applications residing on quarantined desktops associated with desktop moving to NMCI and server/system remaining in legacy.

2. Reduce security vulnerabilities by transitioning the legacy systems into the NMCI enclave.
3. Eliminate duplicate infrastructure costs that are inherent in maintaining legacy networks while NMCI is operational.

The entry point into the Legacy System Transition Process is a FAM-approved system. The CDA should first check the DADMS database for the latest list of approved Navy Enterprise Applications.

The next step is to determine whether the system has an accreditation package: NSCAP and DITSCAP. Before the legacy system can transition to NMCI, it must first receive NMCI DAA approval.

To trigger EDS business contractual process, the Claimant group will order a CLIN 27/CLIN 29. The ST-ERQ is the first step in completing the paperwork for the CLIN requirement. The CLIN 29 services range in scope from network support to full systems operational support.

Prior to system transition, the candidate system's engineered solution and transition plan will pass through the ECCB for review and final approval. The ECCB, comprised of both Navy and EDS representatives, meets on a regular basis to review and approve system and enterprise changes. The goal of the ECCB is to provide situational awareness in NMCI security.

For an in-depth understanding of Risk Mitigation & System Transition, please reference the Legacy System Transition Guide (LSTG).

4.8 PRE-DEPLOYMENT

The Pre-Deployment process is primarily an EDS responsibility. In this stage, the final preparations are made before actual delivery of user seats. Figure 4-13 shows the Pre-Deployment process.

There are several milestones in the Pre-Deployment process that must be met before the Legacy Applications Deployment Readiness Activity (LADRA) can commence:

- The Enterprise B1 is in place at the NOC.
- The Enterprise B2 and GPO are deployed.
- The Application Deployment Solution Instructions are ready.
- The local load applications are ready.
- The NOC is ready to "push" applications to seats. In order to accomplish this, the Radia Instances must be loaded from the EDSL to the San Diego NOC and uploaded to the designated NOC for deployment of the Legacy Applications to the site. For the deployment to the seat to occur, the Transition Team must create the User Profiles in the Active Directory. The Transition Team uses the Application Mapping and creates User Profiles in the Active Directory.
- The PDM has provided the SSE team with the following information:
    - LADRA location
    - Application Mapping
    - Site specific POCs

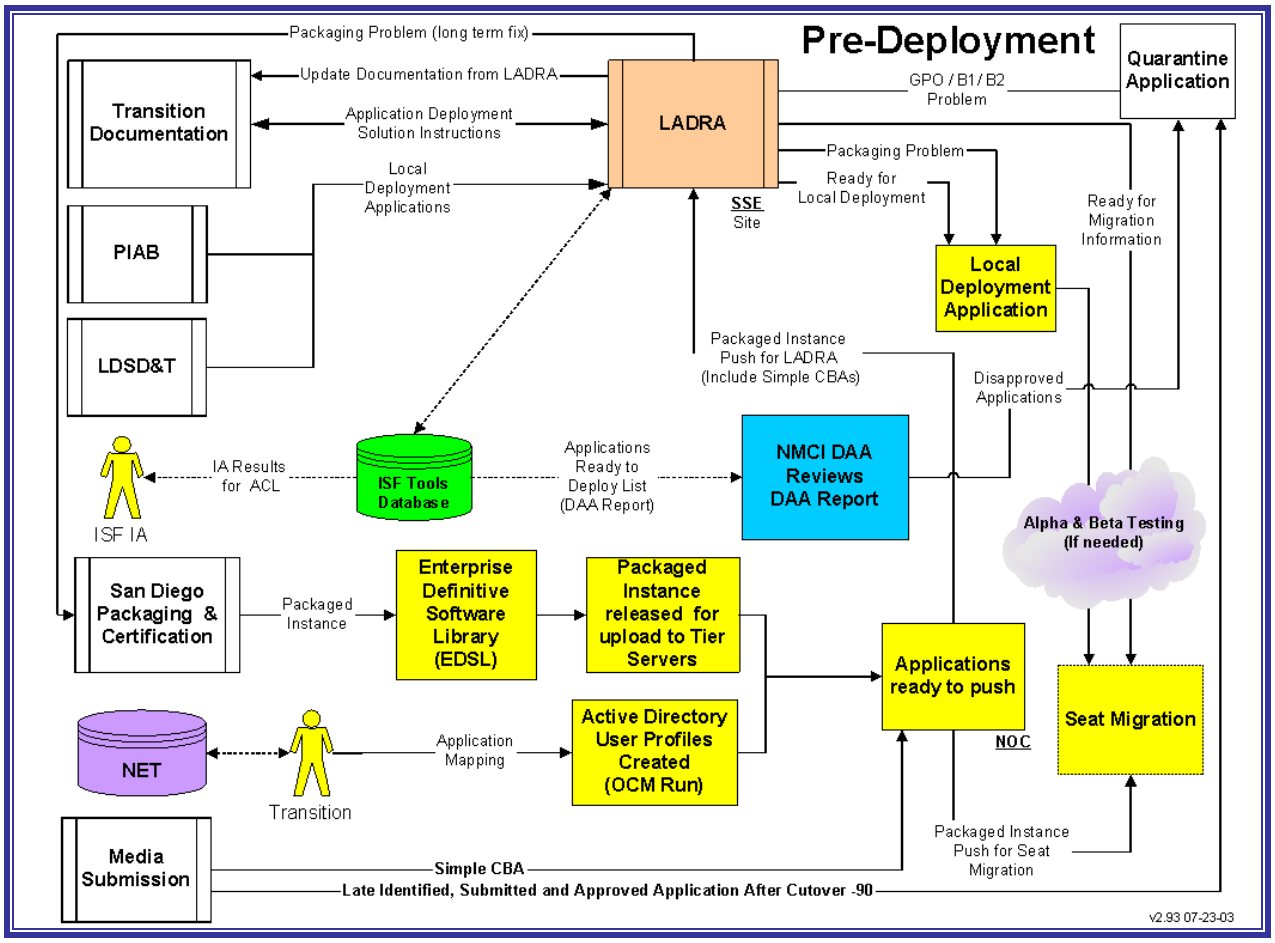


Figure 4-13. Pre-Deployment

The Pre-Deployment test is LADRA. The LADRA sub-process is detailed in Section 4.8 of this guide.

Upon successful completion of LADRA, the Legacy Applications are ready for the initial seat migration (Cutover).

NOTE: During the Pre-Deployment process, the testing and certification status is recorded and tracked in the ISF Tools Database by the SSE team.

4.8.1 Legacy Applications Deployment Readiness Activity (LADRA)

LADRA is the final pre-Cutover testing planned for all Legacy applications. LADRA is not a substitute for Alpha/Beta testing but rather a means of testing Legacy Applications' final configurations, NOC connectivity, boundary policies and migration processes and documentation prior to Cutover. LADRA must not be confused with LDSD&T. Though the SSE team may combine the two steps to provide one seamless and complete test for the customer, the distinct and separate steps of each process must not be skipped. Figure 4-13 depicts LADRA.

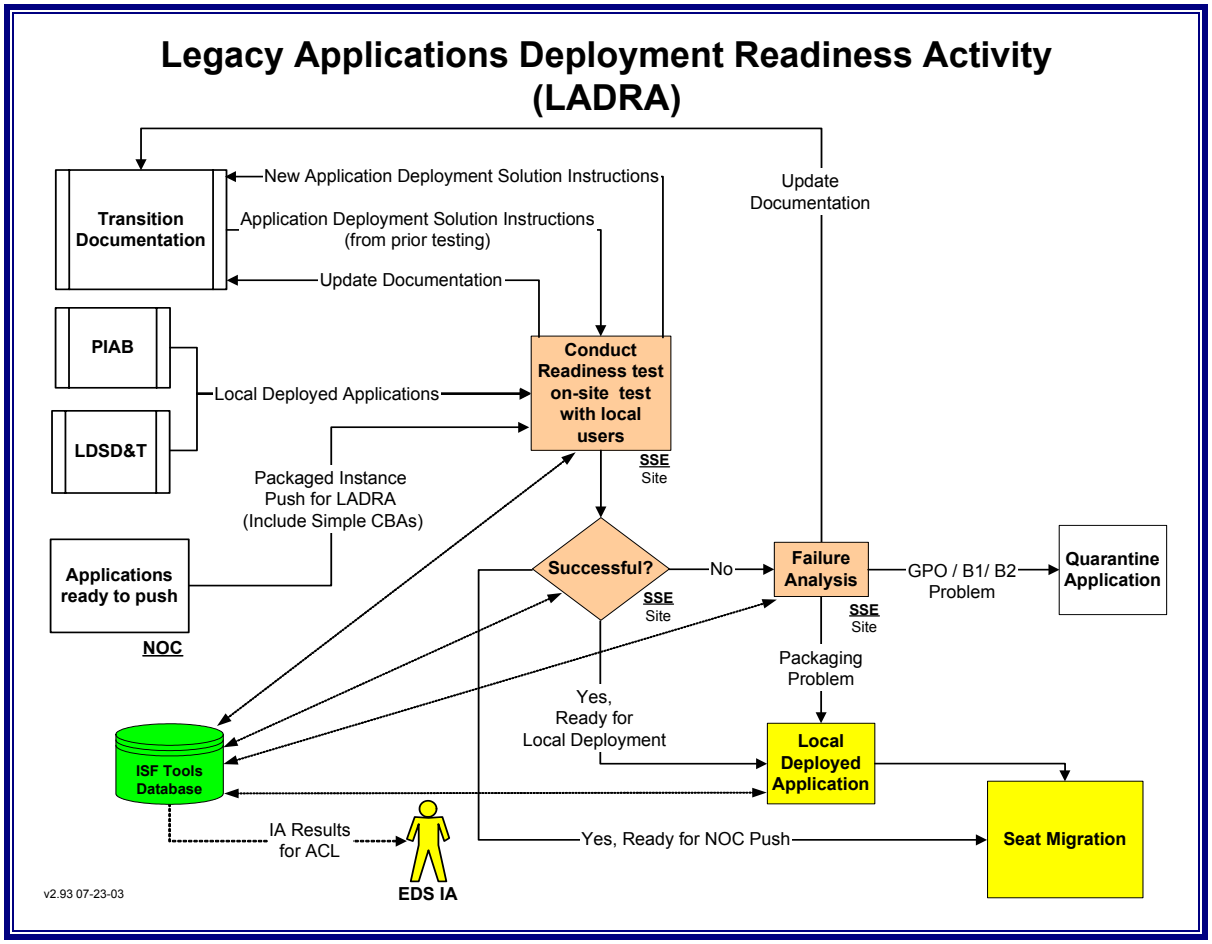


Figure 4-14. Legacy Applications Deployment Readiness Activity (LADRA)

EDS conducts LADRA testing in the live NMCI environment. The goal of LADRA is to test 100% of the applications to be deployed to NMCI on NMCI unclassified and classified seats. These applications must be on the Rationalized List; i.e., have an RFS and be assigned to an Implementation Group (IG). In some instances, testing all applications may not be practical. The LADRA test is designed to verify the transition solutions for the Legacy Applications. The objectives of LADRA are to:

- Verify that the network, firewall configuration, and client/server communications operate properly.
- Evaluate the performance and IA policies of Certified EDSL Legacy Applications. This can include unclassified/classified COTS and GOTS in a true NMCI production environment.
- Provide on-the-job-training for select NMCI Desktop Deployment and EDS Base Ops personnel on the manual configuration of Legacy Applications.
- Ensure proper network configuration and operation.
- Evaluate migration tools.
- Evaluate Radia applications management.
- Validate migration implementation plan.
- Test print functions.

Test seats are set up for LADRA, and the NOC pushes the Legacy Applications to these seats. The EDS SSE and Transition Teams verify that the "push" occurred properly and that the applications installed. Any manual configuration changes needed for the proper installation of an application are noted and analyzed. If these configuration changes can be integrated into the Radia Instance, the application may be rejected and sent back for repackaging and NMCI Certification. If the application must be sent back for repackaging and Certification, it will be deployed locally to prevent any delay to the rollout. The packaging problem will be fixed at a later time.

The application owner/user may be asked to come to the test area to accomplish some usability tests in order to verify that an application is working properly and that it can access the server, datashare, or required Web site.

Applications can fail LADRA for the following:

- Packaging problem – kept on-site and becomes a locally deployed application.
- Connectivity error (B1 or B2) – Quarantined.
- GPO error – Quarantined.
- No user/tester support for application testing – Quarantined.
- Unresolved live network / application interface problems – Quarantined.

Any application failures are documented and the information is recorded in appropriate Transition Documentation.

All applications that successfully complete LADRA testing are ready for Local Deployment or NOC Push to Seat Migration (Cutover).

NOTE: During the LADRA process, the testing and certification status is recorded and tracked in the ISF Tools Database by the SSE team.

4.8.2 Quarantine

Some Legacy Applications will fail to successfully deploy into the NMCI environment during the Rapid Certification Phase of the Legacy Application Transition Process due to their non-compliance with DoN/DoD security, NMCI environmental requirements, DoN policies, etc. An option to continue usage of a failed application is to quarantine it. This means that the application is available for use on a legacy workstation connected to the legacy network. Quarantined applications will not be allowed to operate in the NMCI environment unless a solution is engineered or a waiver can be obtained to allow then to operate in the NMCI environment. This waiver may be permanent (such as a boundary change), or temporary (such as a waiver granted to allow for a new solution to be engineered). Quarantined applications may continue to operate in the legacy environment while they are evaluated for NMCI-compatible solutions.

Reasons for quarantine include:

- Administrative Failures:
  - NMCI Ruleset Kills that were falsely Quarantined
  - Late Submission
  - Incomplete Package Submission (Missing RFS, User, Password or Media)
  - Lack of User Support During Testing

- Technical Failures:
  - Windows 2000 Incompatibility
  - Gold Disk Interoperability
  - Deployment Failure (Network Connectivity, unsuccessful load, etc.)
  - Enterprise Group Policy Object Constraints
  - Violation of Enterprise Boundary (B1/B2) Policy

4.8.2.1 Quarantine Implementation Strategy

The following guidelines are provided (not mandated) to help determine deployment solutions for quarantined applications based on user usage:

- Less than 1 hour per user per day = 7 users per machine
- Greater than 1 hour, but less than 3 hours per user per day = Negotiation between CTR/EDS/RIL
- Greater than 3 hours per user per day = Dual workstation (dual desktop)
- Further considerations: Physical space for workstations, location of users, heating, ventilation, air conditioning (HVAC), power requirements, etc.

Because requirements vary between sites, deployment solutions will be done site-by-site. Actual requirements and solutions are determined through negotiations between the Site CTR, EDS Site Manager and PMO RIL.

4.8.2.2 Quarantine Remediation

IATT is responsible for taking the lead in remediation of quarantined applications, that are identified by EDS in the DAA report for technical failures. Technical failures are identified as: Boundary Failures, GPO Failures, W2K Failures and technical issues/problems identified during LADRA testing. The IATT, Echelon II Command, Command/Site, EDS and CDAs will conduct a thorough assessment of the quarantined applications and identify the required actions for NMCI transition as deemed appropriate following the NMCI DAA, Navy IO, and specific Site prioritization strategies. The IATT will provide guidance and test results to the Command/Site/CDA for the development of documentation required for transition of the application into the NMCI network. During the Quarantine Remediation process, IATT records and tracks the testing and certification status of applications/systems which have failed for technical reasons, in their database in the form of a Quarantine Desktop Application Transition Strategy or (QDATS).

The Quarantine Remediation principles apply to all applications and systems that have been quarantined as a result of the NMCI Legacy Applications Rapid Certification process. There is a prioritization step to identify those high priority applications that will be resolved by the IATT. Application/system priority are set for in the NETWARCOM Admirals Most Wanted List, Applications/Systems that cause significant dual desktop situations and applications/systems deemed priority by the NMCI PMO. All remaining quarantined application resolutions are the responsibility of the appropriate Echelon II Command.

The following process serves as a tool to assist IATT, Echelon II Command, Command/Site, EDS, and the CDA with the evaluation of applications and systems that support the organization's vision, mission, and goals, while transitioning to NMCI. The process begins with prioritization via the various reports and lists that identify the applications that have failed to deploy to the NMCI environment. This process

concludes with successful deployment or discontinued use of all quarantined applications. The IATT Quarantine Application Lead, will oversee the execution of this effort with the IATT Quarantine Remediation Team (QRT), working with Echelon II Commands, CDA and Sites in the execution of these processes.

5.0 CONCLUSION

The transition of Legacy Applications is essential to the successful implementation of NMCI. This is a monumental task requiring maximum coordination between the DON and EDS. Every member of the DON, PMO, PEO-IT, and EDS must be committed to the success of this endeavor. It is also critical for NMCI customers to begin identification and collection of Legacy Applications and their data as early as possible in the process. Customers should also begin the process of rationalization and prioritization as soon as practicable.

The goal of the Legacy Applications process is to ensure that customers will have continued access to their critical applications after the transition to NMCI. The efforts outlined in this document will be resource-intensive, so it is imperative that NMCI customers allocate the appropriate personnel to accomplish this goal. NMCI is the accepted solution of the DON and promises a uniformly higher level of security, improved standardization, and reduced duplication, redundancy, and software support costs.

5.1 LIST OF RESOURCES

The definitive EDS source for customers interested in the transition of legacy application is http://www.nmci-isf.com/transition.htm.

POCs:

- SPAWAR Program Management Office – 858-537-0399
- SPAWAR Program Management Office – 619-524-7435
- Marine Corps Program Management Office – 703-784-3788 (DSN 278)
- Electronic Data Systems (EDS) – 619-817-3487
- Applications Enterprise Action Group (AEAG) – 703-607-5653, 703-607-5654
- NEADG (for developers and CDAs) – 858-826-5168

APPENDIX A – LEGACY APPLICATIONS POA&M TEMPLATE

	SITE	IATT	EDS	NMCI DAA	NADTF	PMO	ECHELON II CIO
SITE PREPARATION							
APPOINT LEGACY APPLICATIONS POC/MANAGER	CO						
Identify Classified requirements							
OBTAIN LEGACY APPLICATIONS TRANSITION GUIDE (LATG) FROM EDS WEBSITE & REVIEW	CO, CIO, LAPOC, CTR						
ESTABLISH CONTACT WITH PMO/EDS	LAPOC						
Obtain Process Brief from PMO							
Meet EDS SM at AOR							
ESTABLISH TOOLS DATABASE ACCESS							
Contact Echelon II Command for Access	LAPOC						
OBTAIN TOOLS DATABASE TRAINING							
Download Database Users Guide (fm website)							
If required, obtain training from Echelon II POC, EAGLE DMT, NMCI Help Desk							
ONSITE TEST FACILITY PLANNING							
DETERMINE FACILITY REQUIREMENT FOR EDS TESTING			SM				
ACQUIRE LOCAL IATO FOR TESTING CONNECTIVITY	Site DAA		SM				
REVIEW, ACCEPT & ASSIGN PIAB OR LADRA FACILITY PLAN			SM				
IDENTIFICATION							
CREATE IDENTIFICATION & RATIONALIZATION GAME PLAN	LAPOC						
SOCIALIZE SITE'S GAMEPLAN AND STRATEGY	LAPOC						
SURVEY USERS FOR GOTS & COTS REQUIREMENTS							
COMPARE SURVEY RESULTS AGAINST APP CATALOG IN ISF TOOL							

	SITE	IATT	EDS	NMCI DAA	NADTF	PMO	ECHELON II CIO
SELECT THOSE APPS FOUND IN APP CATALOG							
ENTER APPS NOT FOUND IN APP CATALOG IN CMD/SITE RECORD							
CREATE USER-LIST; BEGIN AM							
ENTER DATA IN NET							
IDENTIFY/DEFINE/CREATE SITE LOADSETS							
GATHER IN-USE PERIPHERALS, DRIVERS, SUPPLEMENTARY APPS							
COMPLETE RAW PERIPEHRAL & DRIVER LIST							
COMPLETE RATIONALIZED PERIPHERAL & DRIVER LIST							
SUBMIT RATIONALIZED PERIPHERAL & DRIVER LIST TO EDS SM							
IDENTIFY LEGACY APPLICATIONS SERVERS							
SUBMIT DATA TO EDS SM							
IDENTIFY DATASHARE/REACHBACK REQUIREMENTS							
SUBMIT DATA TO EDS SM							
RATIONALIZATION							
DERIVE RAW APPLICATION LIST							
CATEGORIZE APPS BY TYPE AND FUNCTIONALITY							
REMOVE SIMPLE/DEVELOPER APPS FROM TOOLS DB LIST							
APPLY NMCI APPICATION RULESET (TO NON-DEVELOPER APPS)							
PERFORM COTS & GOTS RATIONALIZATION							
APPLY AVAILABLE STANDARDS							
APPLY APPLICATION MAPPING							
COLLECTION							
COLLECT MEDIA (NO MEDIA FOR CBA APPLICATIONS)							
COLLECT INSTALLATION INSTRUCTIONS AND TEST SCRIPTS							
GENERATE RFS FROM ISF TOOLS DATABASE							

	SITE	IATT	EDS	NMCI DAA	NADTF	PMO	ECHELON II CIO
OBTAIN TEST PLAN							
IDENTIFY/COLLECT LICENSE COPY							
NO LICENSE – OBTAIN LICENSE OR ORDER FROM CLIN23							
IDENTIFY/COLLECT DESKTOP & SERVER CONNECTIVITY (NETWORK DIAGRAM)							
PERFORM FINAL USER/APP/MACHINE/SERVER/PERIPHERAL MAPPING							
SUBMIT TO EDS SM							
FINALIZED RATIONALIZED LIST DUE AT CUTOVER -120							
ECHELON II COMMAND REVIEWS AND APPROVES FINAL ACCEPTED RATIONALIZED LIST							
NADTF SCRUBS FINAL ACCEPTED RATIONALIZED LIST							
KILLED APPLICATIONS REMOVED FROM RATIONALIZED LIST							
FINALIZE LOADSETS							
SUBMIT DATA TO EDS SM							
PREPARE ERQ FOR EACH COMPLEX APPLICATION	RISK MITIGATION	RISK MITIGATION					
SUBMIT TO EDS SM							
GATHER AVAILABLE SSAA, IATO AND DITSCAP DOCUMENTATION FOR IA VULNERABILITY ASSESSMENT	RISK MITIGATION	RISK MITIGATION					
MEDIA SUBMISSION							
FOR NEW APPLICATIONS TO BE CERTIFIED SUBMIT THE FOLLOWING:							
RFS CREATED IN THE TOOLS DATABASE			RECEIPT				
NETWORK DIAGRAM			RECEIPT				
SOFTWARE MEDIA			RECEIPT				
INSTALLATION INSTRUCTIONS AND FUNCTIONAL TEST PLAN			RECEIPT				
FOR CBA APPLICATIONS SUBMIT THE FOLLOWING:							
RFS			RECEIPT				
NETWORK DIAGRAM			RECEIPT				

	SITE	IATT	EDS	NMCI DAA	NADTF	PMO	ECHELON II CIO
FUNCTIONAL TEST PLAN			RECEIPT				
DELIVER MEDIA SUBMISSION PACKAGE TO EDS SM BY CUTOVER -90							
REVIEW SITE'S SUBMISSION PACKAGE FOR COMPLETENESS			SM/SSE				
TESTING (ALL)							
A, SAN DIEGO PACKAGING AND CERTIFICATION			AIT				
AUDIT, PACKAGING, USABILITY TEST, GOLD DISK TESTING,			AIT				
APPLICATION STATUS IS RECORDED AND TRACKED IN TOOLS DATABASE			AIT				
B. COMPLEX APPLICATION LAB (CAL)			AIT				
AUDIT, PACKAGING, USABILITY TESTING, GOLD DISK TESTING			AIT				
			AIT				
APPLICATION STATUS IS RECORDED AND TRACKED IN TOOLS DATABASE			AIT				
C. POP-IN-A-BOX (PIAB)			SSE				
AUDIT, PACKAGING			SSE				
PREPARE LOCAL DEPLOYMENT SOLUTIONS			SSE				
SCHEDULE AND PARTICIPATE IN USABILITY TEST	USER/OWNER		SSE				
PARTICIPATE IN IA TESTING (B1 & B2)	USER/OWNER		SSE				
GOLD DISK TESTING	USER/OWNER		SSE				
APPLICATION TESTING & CERTIFICATION STATUS IS RECORDED AND TRACKED IN TOOLS DATABASE			SSE				
COMPILE & INPUT APPLICATION DEPLOYMENT SOLUTION INSTRUCTIONS			SSE				
D. LOCAL DEPLOYMENT SOLUTIONS DEVELOPMENT AND TESTING (LDSD&T)			SSE				
AUDIT			SSE				
PREPARE LOCAL DEPLOYMENT SOLUTIONS			SSE				
SCHEDULE AND PARTICIPATE IN USABILITY TEST	USER/OWNER		SSE				

	SITE	IATT	EDS	NMCI DAA	NADTF	PMO	ECHELON II CIO
PARTICIPATE IN IA TESTING (B1 & B2)	USER/OWNER		SSE				
GOLD DISK TESTING	USER/OWNER		SSE				
APPLICATION TESTING & CERTIFICATION STATUS IS RECORDED & TRACKED IN TOOLS DATABASE			SSE				
COMPILE & INPUT APPLICATION DEPLOYMENT SOLUTION INSTRUCTIONS			SSE				
USABILITY TESTING							
IDENTIFY AND SCHEDULE A PRIMARY & SECONDARY USER/TESTER	LA POC						
GENERATE ETHERPEEK TRACES; DOCUMENT & STORE RESULTS IN SITE FOLDER			SSE				
PRE-DEPLOYMENT			SSE				
LEGACY APPLICATIONS DEPLOYMENT READINESS ACTIVITY (LADRA)			SSE				
CONDUCT READINESS TEST WITH LOCAL USERS	USER/OWNER		SSE				
FAILURE ANALYSIS	USER/OWNER		SSE				
CREATE APPLICATIONS READY TO DEPLOY LIST (WEEKLY)			SSE				
REVIEW APPLICATIONS READY TO DEPLOY LIST (WEEKLY)							
PACKAGE INSTANCE LOADED TO EDSL							
PACKAGE INSTANCE UPLOADED TO TIER SERVERS							
CREATE ACTIVE DIRECTORY USER PROFILES							
APPLICATIONS READY TO PUSH/LOCAL DEPLOY							
TESTING & CERTIFICATION STATUS IS RECORDED AND TRACKED IN THE TOOLS DATABASE							
SEAT MIGRATION (ROLLOUT)							

APPENDIX B – NMCI STANDARD SEAT SERVICE (GOLD DISK) CONTENTS & NAVY ENTERPRISE STANDARDS

The following table is the contents of the NMCI Standard Seat Services (Gold Disk) at the time this guide was published. To obtain the latest Gold Disk Contents, see http://www.nmci-eds.com/downloads/Gold_disk_contents.pdf

NMCI

Gold Disk Contents

Date Posted: 6/02/03

Gold Disk Contents		
SERVICE	**SOFTWARE DESCRIPTION (MINIMUM VERSION)**	**VENDOR**
Basic		
Operating System	MS Windows 2000 SP3	Microsoft
Office Suite	Standard Office Automation Software Included on the Gold Disk: • MS Word • MS Excel • MS PowerPoint • MS Access	Microsoft
Desktop Management	Diskeeper 7.0413	Executive Software
Email Client	MS Outlook 2000	Microsoft
Internet Browser	Internet Explorer MS 5.5 SP-2 128bit	Microsoft
Virus Protection	Norton A/V Corp Edition v7.5	Symantec
PDF Viewer	Acrobat Reader v5.05	Adobe
Terminal Emulator - Host (TN3270, VT100, X-Terminal)	Reflection 8.0.5 – Web Launch Utility	WRQ
Compression Tool	WinZip v8.1	WinZip
Collaboration Tool	Net Meeting v3.01 (4.4.3385)	Microsoft
Multimedia	RealPlayer 8 (6.0.9.450)	RealNetworks
Multimedia	Windows Media Player v7.01.00.3055	Microsoft
Internet Browser	Communicator 4.76	Netscape
Electronic Records Mgmt	Trim Context	Tower
Plug-ins		
Web Controls	Macromedia Shockwave v8.0	Macromedia
Web Controls	Flash Player 5.0	Macromedia
Web Controls	Apple QuickTime Movie and Audio Viewer v 5.0	Apple
Web Controls	iPIX v6,2,0,5	Internet Pictures
Security Apps		
Security	Intruder Alert v3.6	Symantec
Security	ESM v5.1	Symantec
Agents		
Software Management	Radia Client Connect v.2.1	Novadigm
Inventory, Remote control	Tivoli TMA v3.71	IBM/Tivoli

Version 6.0 1 NMCI 10001.01.UE0

Gold Disk Contents		
SERVICE	**SOFTWARE DESCRIPTION (MINIMUM VERSION)**	**VENDOR**
Remote Connectivity (Notebooks)		
Dial-up connectivity	PAL v4.3	MCI/WorldCom
VPN	VPN Client v4.1	Alcatel

Gold Disk Contents Document Revision History

Version	Date Posted to Web	Item	Revision
1.0	03/01/02	MS Office Suite	Old: MS Office Pro 2000 SR-1a New: Standard Office Automation Software Included on the Gold Disk MS Word MS Excel MS PowerPoint MS Access
2.0	9/19/02	Operating System	Old: MS Windows 2000 Build 2195 SP1 New: MS Windows 2000 Build 2195 SP2/SRP1
		Internet Browser	Old: Internet Explorer MS 5.5 SP-1 128 bit New: Internet Explorer MS 5.5 SP-2 128 bit
		PDF Viewer	Old: Acrobat Reader v.4.05c New: Acrobat Reader v. 5.05
		Terminal Emulator	Old: Reflection 8.0.5 New: Reflection 8.0.5 – Web Launch Utility
		Compression Tool	Old: WinZip v8 New: WinZip v8.1
		Multimedia	Old: Windows Media Player v7.00.1956 New: Windows Media Player v7.01.00.3055
		Electronic Records Management	Old: Trim Captura v4.3* New: N/A
		Web Controls	Old: Apple QuickTime Movie and Audio Viewer v4.12 New: Apple QuickTime Movie and Audio Viewer v5.0
		Software Management	Old: Radia Client Connect New: Radia Client Connect v2.1
		Dial-Up Connectivity	Old: PAL New: PAL v4.1.1.306
		VPN	Old: VPN Client New: VPN Client v3.0
3.0	1/23/03	Electronic Records Management	Old: N/A New: Trim Context

Version	Date Posted to Web	Item	Revision
4.0	2/19/03	Dial Up Connectivity	Old: PAL v4.1.1.306 New: PAL v4.3
		VPN	Old: VPN Client v3.0 New: VPN Client v4.1
5.0	4/9/03	Security	Old: Intruder Alert 3.5 New: Intruder Alert v3.6
6.0	6/02/03	Operating System	Old: MS Windows 2000 Build 2195 SP2/SRP1 New: MS Windows 2000 SP3
		Desktop Management	Old: N/A New: Diskeeper 7.0413 Executive Software
		Security	Old: Intruder Alert v3.6 Axent New: Intruder Alert v3.6 Symantecc
		Security	Old: ESM v5.1 Axent New: ESM v5.1 Symantec

Standardize Application List

http://cno-n6.hq.navy.mil/navcio/leg_apps.htm

Application	Status	Family**	Implementation	Version	NCARP 20 Aug 2002	CLIN 23 Price/Mo
Accelio Capture Classic Form Flow	CLIN 23	ADMIN	All Seats	Starter Kit		$5.47
AutoCAD LT	CLIN 23	ADMIN	All Seats	2002		$49.11
Automated Travel Order System (ATOS) Plus	Standardized	FINANCIAL		040-05.04.05 or 5.4.5	040-05.04.05 (2)	
Automated Travel Order System (ATOS) Plus Traveler	Standardized	FINANCIAL		042-01.01.03		
Field Alcohol and Drug Management Information System for the CAAC/ATF (ADMITS - CAAC/ATF)	Standardized	MAN&PER		2.0	(2)	
Field Alcohol and Drug Management Information System for the DAPA/SACO (ADMITS - DAPA/SACO)	Standardized	MAN&PER		1.2.3		
Aircraft Inventory Readiness and Reporting System (AIRRS)	Standardized	LOG		2.01	No Version (1)	
Aviation Management Supply and Readiness Reporting (AMSRR)	Standardized	LOG		2.0	(1)	
Automated Weight and Balance System (AWBS) *	Standardized	LOG	Run 8.1now, 9 in 20 April 02	8.1 Now, 9.0 Later	(1)	
Aviation Material Maintenance Management (AV3M)	Standardized	LOG		004-14.00.00		
Career Information Program Management (CIPM) 99	Standardized	MAN&PER		1.0d-5	1.0c (1)	
CITRIX ICA Client	Standardized	ENT		6.30.1050		
Computerized Self Evaluation Checklist (CSEC) *	Standardized	C4	1.1 now, 2H, 2K in July 02	1.1 upgrade to 2H, 2K in July 02		

Application	Status	Family**	Implementation	Version	NCARP 20 Aug 2002	CLIN 23 Price/Mo
Defense Automatic Addressing System Center Automated Message Exchange System (DAMES) *	Standardized	LOG		2.11.046		
Defense Property Accountability System (DPAS) Report Viewer*	Standardized	C4		15.0.14	(2) Version 15	
Defense Property Accountability System (DPAS) Report Designer *	Standardized	C4		15.0.14		
DPAS MyEureka *	Standardized	FINANCIAL	Works with DPAS	6.1.313		
DPAS Supra NT	Standardized	LOG	Works with DPAS	8/31/1998		
Distributed Plain Language Address Verification System (DPVS)	Standardized	C4		6.0	6.0(2)	
Electronic Personnel Security Questionnaire (EPSQ)	Standardized	READ		2.2	(1)	
eRoom	CLIN 23	Admin		5.4		
Fund Administration and Standardized Document Automation (FASTDATA)	Standardized	FINANCIAL		2-2	(1) No version	
FEDLOG *	Standardized	LOG		5.1	4.2 (1) /Apr-02 (2)	
Fleet Awards Program	Standardized	ADMIN	Interim	4.2	(1)	
Global Air Transportation Execution System (GATES)	Standardized	LOG		2.06.01		
Global Transportation Network (GTN)	Standardized	LOG		https://www.gtn.transcom.mil/public/home//main/index.html		
Hazardous Material Information System (HMIS)	Standardized	LOG		DEC2001	(1)	

Application	Status	Family**	Implementation	Version	NCARP 20 Aug 2002	CLIN 23 Price/Mo
Hazardous Substance Management System (HSMS)	Standardized	LOG		2.4.X	2.4(2)	
Installation Readiness Reporting System (IRRS) *	Standardized	READ		2.0.1	(2)	
Joint Air Logistics Info System (JALIS)	Standardized	LOG		2.0		
Joint Federal Travel Regulation (JFTR)	Standardized	ADMIN	CD or Web and Adobe Acrobat v5	Folio Viewer v 4.2	3.1A (Vol. I #745, Vol. II #429) (1)	
Microsoft FrontPage	CLIN 23	ADMIN	All Seats	2000		$5.73
Microsoft Publisher	CLIN 23	ADMIN	All Seats	2000		$5.58
Microsoft Project	CLIN 23	ADMIN	All Seats	2000		$14.18
NAVFIT 98A	Standardized	MAN&PER		2.002.0023	2.002.0021 (1)	
Naval Reserve New Order Writing System (NOWS)	Standardized	MAN&PER		1.0		
Navy Drug Screening Program (NDSP)	Standardized	MAN&PER		5.0	5.0 (1)	
Navy Electricity and Electronics Training Series (NEETS)	Standardized	T&E		1.0	(1)	
Navy-Portable Flight Planning (N-PFPS)	Standardized	Weapons Planning		3.2		
Navy Standard Integrated Pay System (NSIPS)	Standardized	FINANCIAL		0.2	(2)	
Norton Utilities	CLIN 23	ADMIN	All Seats	2002		$2.76
Physical Readiness Information System (PRIMS) *	Standardized	MAN&PER	Valid until 31 Mar 03	1.0.11	1.011 (1)	
Physical Readiness Information System Web (PRIMS) *	Standardized	MAN&PER	Web Version Effective 1 Oct 02	1.0		
Readiness Maintenance Stores for Win (RMSWin)	Standardized	LOG		8.0		

Application	Status	Family**	Implementation	Version	NCARP 20 Aug 2002	CLIN 23 Price/Mo
Sierra Hotel Aviation Reporting System (SHARP) *	Standardized	READ		4.1	(1)	
SNAP Automated Medical System (SAMS)	Standardized	MED		25.08.02.00	8.02 (2)	
Standard Account Reporting System Host on Demand (STARS-HOD)	Standardized	ACQ		6.03	5.0.4 (1)	
Standard Automated Logistics Tool Set (WINSALT) *	Standardized	LOG	IATO Nov 02, WINSALT 5.1 once certified	4.17	4.17 (2)	
Standard Labor Data Collection and Distribution Application (SLDCADA)	FAM Consideration	MAN&PER		21.4-XX Multiple Versions (1)(2)(3)	(1) No version	
Stock Control System (SCS)	Standardized	LOG		https://www.scsweb.day.dis.mil		
Turbo Prep	Standardized	C4		2.02A-5N Patch A	(2)	
Visio Professional	CLIN 23	ADMIN	All Seats	2000		$16.13
Visual Basic Professional	CLIN 23	ADMIN	Used with CLIN 0038AA, and CLIN 0038AB	6.0		$23.49
Visual Interdev Professional	CLIN 23	ADMIN	Used with CLIN 0038AA, and CLIN 0038AB	6.0		$23.49
WINATOS	Standardized	FINANCIAL		045.01.00.00		
Window Program Analysis Tool Kit (WINPAT 5.2)	Standardized	FINANCIAL		5.2		

* Implies frequent version updates. As long as the updated version (higher version number) is certified for NMCI, it can be loaded on the network.

** Functional assignments represent ISF Tool or NADTF assignments

APPENDIX C – LATE APPLICATION IDENTIFICATION AND SUBMISSION PROCESS

The Late Application Identification and Submission process is a Navy responsibility, extracted from the CNO messages of 03 Aug 2001 (031345Z AUG 01), 31 Aug 2001 (312137Z AUG 01), 25 Feb 2002 (252250Z FEB 02), and 30 Sep 2002 (301245Z SEP 02).

The 30 Sep 2002 message (301245Z SEP 02) from the Navy Information Office directs all Echelon II Commands to ensure that their Final Rationalized Lists of all NMCI applications (at headquarters and all subordinate Commands) are reflected in the ISF Tools Database within sixty days of the date time group of this message (29 November, 2002). Subsequent additions to the Rationalized List require the approval of the applicable FAM and Navy IO (NADTF).

The 25 July 2003 message (252230Z JUL 03) from the Chief of Naval Operations addresses the strategy for managing Navy applications and databases within NMCI. The message directs all commands commencing NMCI cutover after 1 October 2003 to limit authorized applications to those designated as FAM "approved" or "allowed with restrictions".

This sub-process is a part of the Identification and Rationalization, Collection and Media Submission processes.

There are four combinations of legacy application identification and submission:

- An application is identified and added to the ISF Tools Database before Cutover -120 and submitted before the Command/Site specific media submission deadline Cutover -90.
- An application is identified after the Cutover -120 deadline, but it is submitted before the Command/Site specific media submission deadline Cutover -90.
- An application is identified and added to the ISF Tools Database and Rationalized List before the Cutover -120 deadline, but it is submitted after the Command/Site specific media submission deadline Cutover -90.
- An application is identified after the Cutover -120 deadline, and it is submitted after the Command/Site specific media submission deadline Cutover -90 but prior to the start of Cutover.

NOTE: A legacy application's late status will jeopardize its ability to be included in the initial seat migration with those legacy applications that were not identified late.

Command/Sites' Identification Deadlines: (Per CNO message of 30 Sep 2002)

All Echelon II Commands will ensure that their Final Rationalized Lists of all NMCI applications (at headquarters and all subordinate Commands) are reflected in the ISF Tools Database by 29 November 2002.

Subsequent additions to the Rationalized List require the approval of the applicable FAM and Navy IO (NADTF).

Sites Actions and Consequences

Here is what happens for each identification and submission combination:

- Identified and Submitted On-Time - An application is identified and added to the ISF Tools Database before the Cutover -120 deadline and submitted before the Command/Site specific media submission deadline Cutover -90:
    - This is what should happen as part of the normal legacy applications transition process. The application continues through the process with no modifications or consequences.
- Identified Late and Submitted On-Time - An application is identified after the Cutover -120 deadline, but it is submitted before the media submission deadline Cutover -90:
    - For this Late Identified Application, the Command/Site can enter the application into the Command/Site record in the ISF Tools Database. The application will automatically be marked as late when it is added after the Cutover -120 deadline. The application will not be added to the Applications Catalog or the Rationalized List until an approved waiver is received from the FAM and NADTF.
    - An application identified late has to be approved by the Echelon II Command. If the Echelon II Command wants the application added to the rationalized list, it must be identified to the Navy CIO (FAM & NADTF) via official Navy message. If the Echelon II Command does not approve the application, the application is rejected and removed (unrationalized) from the FRL by the Echelon II Command.
    - If the Navy CIO (NADTF) and the FAM approve the application, the FAM will post a status report on waivers on the DADMS website, indicating that the application is approved as "late." The FAM will mark the application as "Accepted" in the ISF Tools Database. The application will move above the "line" in the Rationalized List. The application will be Quarantined and continue through the process, to be certified and processed into NMCI at a later date. If the FAM does not approve the application, they will mark the application "Disapproved" in the ISF Tools Database and the application will not transition into NMCI.

NOTE: A rejected or Killed application will not be utilized in NMCI and **will not** be Quarantined.

- Identified On-Time and Submitted Late - An application is identified and added to the ISF Tools Database and the Rationalized List before the Cutover -120 deadline, but it is submitted after the Command/Site specific media submission deadline Cutover -90:
    - For this Late Submitted Application, EDS, upon receiving it, will indicate the application was received late in the ISF Tools Database after Cutover -90 by marking the Late Column with a "Y" for yes and showing the entry as red.
    - The responsible Echelon II Command for the site transitioning to NMCI must approve an application identified on time but submitted late. If the Echelon II approves the application for late submission, it must be forwarded by official Navy message to the Navy CIO (FAM) for final adjudication. If the Echelon II Command does not approve the application, the application is rejected and removed (unrationalized) from the FRL by the Echelon II Command.
    - If the Navy CIO (FAM) approves the application, the FAM will post a status report on waivers on the DADMA website. The FAM will mark the application as "Accepted" in the ISF Tools Database. The application will be Quarantined and continue through the process, to be certified and processed into NMCI at a later date. If the Navy CIO does not approve the application, the FAM will mark the application

"Disapproved" in the ISF Tools Database and the application will not transition into NMCI.

NOTE: A rejected or Killed application will not be utilized in NMCI and **will not** be Quarantined.

- Identified Late and Submitted Late - An application is identified after the Cutover -120 deadline, and it is submitted after the media submission deadline Cutover -90 but prior to the start of Cutover:
  - For this Late Identified Application, the Command/Site can enter the application into the Command/Site record in the ISF Tools Database. The application will automatically be marked as late when it is added after the Cutover -120 deadline. The application will not be added to the Applications Catalog or the Rationalized List until an approved waiver is received from the FAM.
  - An application identified late and submitted late must be approved by the Echelon II Command. If Echelon II approval is given for the late identification/submission, it must be forwarded by official Navy message to the Navy CIO (FAM) for final adjudication. If the application is not approved by the Echelon II Command, the application is rejected and removed (unrationalized) from the FRL by the Echelon II Command.
  - If the Navy CIO (FAM) approves the application, the NADTF will post a status report on waivers on the DADMS website indicating that the application is approved as "late." The FAM will mark the application as "Accepted" in the ISF Tools Database. The application will move above the "line" in the Rationalized List. The application will be Quarantined and continue through the process, to be certified and processed into NMCI at a later date. If the FAM does not approve the application, they will mark the application "Disapproved" in the ISF Tools Database and the application will not transition into NMCI.

NOTE: A rejected or Killed application will not be utilized in NMCI and **will not** be Quarantined.

Applications identified and/or submitted after the start of Cutover are determined to be "emergent." Emergent applications are not considered to be legacy applications based on the NMCI contract terms. The Site and/or the Echelon II Command will be responsible for the financial implications associated with their NMCI Certification and seat migration for emergent applications. Emergent applications are handled in accordance with the NMCI Release Development and Deployment Guide (NRDDG).

Changes to Legacy Applications Prior to Cutover

Changes (Updates, Patches, Mods, Upgrades, Revisions, Fixes, etc.) to Legacy Applications will be accepted and implemented by EDS prior to Cutover -45. Changes submitted after Cutover -45 would cause the entire application to be Quarantined until the change can be successfully processed. This applies only to those original applications that were in the ISF Tools Database and on the Final Rationalized List. Processing of these changes can occur once EDS has sufficient resources available during or after Cutover. Processing these changes will not affect or delay normal rollout.

CDA Identification

All existing Central Design Authorities (CDAs) must have their applications identified and RFS submitted.

Quarantined Applications due to Late Identification and Submission

The standard rule followed by EDS for working on late identified and submitted Quarantined applications is to start processing them 30 days after Cutover Complete. Cutover Complete occurs when the last scheduled seat is rolled. EDS is not required to process a late identified and submitted Quarantined application prior to this time if it will delay the Cutover of the site. However, if EDS has the resources available and Cutover will not be delayed, working on Quarantined applications can occur at any time. This situation is at the discretion of the ISF and is to be negotiated between the Command/Site and EDS.

- **FAM (NADTF) Late Applications Approval Process**
- **Late Identification and Submission Waiver**

Applications that are identified and submitted late will require waiver approval from the appropriate FAM. Waiver Request is available from the FAM (NADTF) DADMS database.

APPENDIX D – PERTINENT NAVAL MESSAGES

NAVAL MESSAGES INDEX

D17. 162010Z JUN 03
MODIFIED IMPLEMENTATION GUIDANCE FOR THE NMCI TRANSITIONAL BOUN
DARY TWO POLICY

D18. 021936Z MAY 03
PRE-AOR INFORMATION ASSURANCE REQUIREMENTS FOR SITE,
/DAA, PMO AND EDS

D19. 021700Z MAY 03
INTERIM APPROVAL TO OPERATE (IATO) THE UNCLASSIFIED
/NMCI TRANSITIONAL BOUNDARY TWO POLICY

D20. 252230Z JUL 03
STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI

D21. 211902Z JUL 03
NMCI PROGRESS

D22. 071455Z AUG 03
NAVY DESIGNATED APPROVAL AUTHORITY ASSUMPTION

D23. 252230Z JUL 03
STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI

D24. 011854Z AUG 03
STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI

D25. 252230Z JUL 03
STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI

D1. Navy CNO Message 252250 Z FEB 02

Prec: ROUTINE

DTG: 252250Z FEB 02

Subj: NMCI LEGACY APPLICATIONS TRANSITION PROCESS//

UNCLAS

MSGID/GENADMIN/CNO N09T/001-02//

SUBJ/NMCI LEGACY APPLICATIONS TRANSITION PROCESS//

REF/A/GENADMIN/CNO 09T WASHINGTON DC/061414ZJUL2001/003-01//

REF/B/GENADMIN/CNO 09T WASHINGTON DC/031345ZAUG01/005-01//

NARR/REFS A AND B ARE NAVY CIO MESSAGES 003-01 AND 005-01 AND PROVIDE GUIDANCE FOR NMCI TRANSITION OF LEGACY APPLICATIONS AND DIRECTED A ONE-TIME INVENTORY AND REPORTING OF LEGACY APPLICATIONS AT ALL ECHELON II COMMANDS.//
POC/ALAND, DAVID/CAPTAIN/OPNAV NAVY CIO/LOC: WASHINGTON DC/TEL: 703-604-6880//

AMPN/EMAIL: ALAND.DAVID@HQ.NAVY.MIL//

RMKS/1. EXECUTIVE SUMMARY. THE TRANSITION OF LEGACY APPLICATIONS TO NMCI IS A CRITICAL STEP FORWARD IN OUR ABILITY TO REALISTICALLY PERFORM INFORMATION RESOURCE MANAGEMENT. IT IS A LEADERSHIP ISSUE WHICH REQUIRES YOUR IMMEDIATE AND DIRECT ATTENTION. STATUS OF EACH ECHELON II COMMAND'S IDENTIFICATION, RATIONALIZATION, AND SUBMISSION OF APPLICATIONS FOR CERTIFICATION AND ACCREDITATION WILL BE REPORTED TO THE CNO AND SECNAV ON A WEEKLY BASIS. THIS MESSAGE BOTH MANDATES THE USE OF THE LEGACY APPLICATION TRANSITION GUIDE (LATG) AND MODIFIES LATG, PROVIDING DETAILED SUBMISSION DATES AND PROCEDURES THAT MUST BE FOLLOWED. THE MODIFICATION OF THE LATG SEPARATES THE NMCI CERTIFICATION PROCESS FROM THE FINAL ACCREDITATION PROCESS AND DELIVERS APPLICATIONS WHICH WILL OPERATE ON NMCI SEATS WITHOUT COMPROMISING SECURITY. REGRET THE LENGTH OF MESSAGE BUT THIS PROCESS CHANGE REQUIRES DETAIL AND CLARITY.

2. ECHELON II COMMANDERS ARE EACH RESPONSIBLE FOR THE IDENTIFICATION, RATIONALIZATION, AND SUBMISSION FOR CERTIFICATION AND ACCREDITATION OF THEIR APPLICATIONS. A CENTRAL DATABASE HAS BEEN ESTABLISHED FOR ALL NAVY APPLICATIONS. ACCESS TO THE DATABASE IS VIA A WEBSITE REQUIRING A USER PASSWORD. A SEPARATE MESSAGE WILL PROVIDE INFORMATION ON HOW ACCESS TO THE DATABASE CAN BE OBTAINED VIA EACH INDIVIDUAL'S ECHELON II COMMAND TO READ AND/OR WRITE TO THE DATABASE. A REVIEW OF THIS DATABASE INDICATES THAT MOST NMCI INCREMENT 1.0 AND 1.5 COMMANDS HAVE NOT COMPLETED THE REQUIRED DATA SUBMISSION IN SUPPORT OF NMCI IMPLEMENTATION. ADDITIONALLY, MOST COMMANDS SCHEDULED FOR NMCI INCREMENT 2.0 AND BEYOND HAVE SUBMITTED INCOMPLETE DATA WHICH COULD IMPACT NMCI IMPLEMENTATION. SITE TRANSITION EXECUTION MANAGER (STEM), ENTERPRISE APPLICATIONS GROUP FOR LEGACY & EMERGING (EAGLE) AND INFORMATION ASSURANCE TIGER TEAM (IATT) PERSONNEL HAVE BEEN FIELDED TO ASSIST TRANSITIONING SITES

WITH THIS TASK. HOWEVER, THE SPEED AT WHICH LEGACY APPLICATIONS ARE IDENTIFIED, RATIONALIZED (REDUCED IN NUMBER), TESTED, CERTIFIED, AND ACCREDITED MUST BE IMPROVED. THERE ARE THREE KEYS TO IMPROVING THIS PROCESS. THE FIRST IS TO ENSURE EACH ECHELON II COMMAND MAINTAINS THEIR APPLICATION DATA CURRENT AND ACCURATE IN THE APPLICATION DATABASE TO ELIMINATE DUPLICATION OF EFFORT ACROSS THE NAVY ENTERPRISE. APPLICATIONS CERTIFIED AND ACCREDITED UNDER THE LATG PROCESS DO NOT REQUIRE DUPLICATE CERTIFICATION AND ACCREDITATION AT SUBSEQUENT COMMANDS/SITES. (REQUEST FOR SERVICE (RFS) SUBMISSION IS STILL REQUIRED BY SUBSEQUENT COMMANDS/SITES TO DOCUMENT APPLICATION USE AND PREVIOUSLY ACCOMPLISHED CERTIFICATION.) THE SECOND KEY IS A REDUCTION IN THE NUMBER OF LEGACY APPLICATIONS ACHIEVED BY ECHELON II RATIONALIZATION AND NAVY TRIAGE PROCESS. (DATA COLLECTED THUS FAR SHOWS APPROXIMATELY 10-20 PERCENT OF ALL APPLICATIONS CURRENTLY CERTIFIED AND ACCREDITED DO NOT HAVE ANY IDENTIFIED USERS, WHICH HAS RESULTED IN A NEEDLESS EXPENDITURE OF SCARCE RESOURCES.) THE THIRD KEY IS A REDUCTION IN THE REQUIREMENTS FOR INCLUDING LEGACY APPLICATIONS AT NMCI SEAT CUTOVER, BUT NOT A REDUCTION IN REQUIREMENTS FOR LEGACY APPLICATION ACCREDITATION. IN ORDER TO REDUCE THE IMPACT TO NMCI SEAT ROLLOUT, THE APPLICATION TRANSITION PROCESS IS MODIFIED PER PARAGRAPH 3 AND ACTION IDENTIFIED IN PARAGRAPH 4 IS MANDATORY.

3. LEGACY APPLICATION TRANSITION PROCESS MODIFICATION. THE FOLLOWING PROCESS MODIFICATIONS ARE EFFECTIVE IMMEDIATELY AND SHALL BE FOLLOWED IN CONJUNCTION WITH THE LATG:

A. GENERAL: THE CURRENT LEGACY APPLICATION PROCESS ENTAILS SITE IMPLEMENTATION VICE COMMAND IMPLEMENTATION DURING THE LEGACY APPLICATION IDENTIFICATION AND THE RATIONALIZATION PROCESSES AND THE COMPLETION OF THE CERTIFICATION PROCESS (COMPATIBILITY WITH THE NMCI OPERATING ENVIRONMENT) AND THE SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA) PRIOR TO COMMENCING CUTOVER OF SEATS. THE NEW PROCESS REQUIRES ECHELON II CHAIN OF COMMAND (COC) INVOLVEMENT DURING THE IDENTIFICATION AND THE RATIONALIZATION PROCESSES AND DIVIDES THE CERTIFICATION PROCESS INTO TWO PHASES, THE NMCI CERTIFICATION PHASE AND THE RISK MITIGATION (ACCREDITATION) PHASE.
B. IDENTIFICATION AND RATIONALIZATION: NEW PROCESS REQUIRES SUBORDINATE COMMANDS TO SUBMIT THEIR RATIONALIZED LIST OF APPLICATIONS VIA THEIR COC TO THEIR ECHELON II FOR RATIONALIZATION ACROSS THE ECHELON II'S ENTERPRISE. IT REQUIRES A WEEKLY REPORTING OF EACH COMMAND'S PROGRESS IN COMPLETING SUBMISSION REQUIREMENTS FOR THE CERTIFICATION PROCESS.
C. NMCI CERTIFICATION: IN THE NEW PROCESS THE NMCI CERTIFICATION PHASE INCLUDES THE DEVELOPMENT OF RATIONALIZED LISTS OF APPLICATIONS, THE SUBMISSION OF REQUESTS FOR SERVICE (RFS) AND MEDIA FOR THOSE APPLICATIONS, THE SUBMISSION OF THE CERTIFICATION PHASE ENGINEERING REVIEW QUESTIONNAIRE (ERQ), THE ACTUAL CERTIFICATION TESTING OF THE APPLICATION, AND THE SUBMISSION OF AN IATT VULNERABILITY ASSESSMENT LETTER TO THE NMCI DESIGNATED APPROVAL AUTHORITY (DAA) (CAPTAIN BOB WHITKOP, COMMANDER NAVY NETWORK OPERATIONS COMMAND (CNNOC)). THE NMCI CERTIFICATION PROCESS CULMINATES IN THE ISSUANCE OF AN INTERIM AUTHORITY TO OPERATE (IATO) LETTER FROM THE NMCI DAA. THE IATO WILL CONTAIN LIMITATIONS ON THE OPERATION OF EACH APPLICATION AND REQUIRE INFORMATION ASSURANCE RISK MITIGATION ACTIONS TO BE ACCOMPLISHED WITHIN TIME SPECIFIED IN PARAGRAPH 3.D.

D. CERTIFICATION PROCESS CHANGES: THE PACING FACTOR FOR MUCH OF THE NMCI CERTIFICATION PROCESS WILL CONTINUE TO RELY ON OBTAINING THE RFS, MEDIA, AND COMPLETION OF THE ERQ FOR EACH COMMAND'S APPLICATIONS AT EACH SITE. IT IS ESSENTIAL THAT BOTH THE APPLICABLE ECHELON II COMMANDS AND THE SITE ENSURE THIS DATA IS SUBMITTED IN A TIMELY MANNER IN ORDER TO SUPPORT THE NMCI IMPLEMENTATION SCHEDULE. THE NMCI CERTIFICATION ERQ AND THE RISK MITIGATION (ACCREDITATION) ERQ INCLUDE ALL THE DATA REQUIREMENTS OF THE ORIGINAL ERQ. HOWEVER, THE NMCI CERTIFICATION ERQ HAS BEEN SIGNIFICANTLY REDUCED IN SIZE AND COMPLEXITY TO EXPEDITE THE SEAT CUTOVER PROCESS, WHILE COLLECTING THE NECESSARY INFORMATION TO ENSURE NETWORK SECURITY IS MAINTAINED AT CUTOVER. THE NMCI CERTIFICATION TESTING HAS ALSO BEEN STREAMLINED. EACH APPLICATION WILL UNDERGO AN ON SITE POP-IN-A-BOX (PIAB) TEST TO ENSURE COMPATIBILITY WITH THE MICROSOFT WIN2K OPERATING SYSTEM, DESKTOP GROUP POLICY OBJECT (GPO), SECURITY COMPONENTS AND SETTINGS. THE PIAB TESTING WILL ALSO PROVIDE CONNECTIVITY REQUIREMENTS BETWEEN CLIENT AND SERVER AT THE PROTOCOL, SERVICE AND PORT LEVEL. ADDITIONAL PERSONNEL AND EQUIPMENT WILL BE ASSIGNED BY THE PMO AND THE NMCI CONTRACTOR TO THE EXISTING TEAMS IN ORDER TO CONDUCT THIS ON SITE PIAB TESTING AND DOCUMENTATION AT A GREATER NUMBER OF SITES CONCURRENTLY. BASED ON THIS INFORMATION GAINED FROM THE PIAB TESTING, THE IATT WILL PROVIDE A RISK ASSESSMENT OF EACH APPLICATION AS FOLLOWS:

-- LOW RISK - COMPLIANT WITH NAVY/MARINE CORPS ENCLAVE PROTECTION POLICY AND ACCREDITED.

-- MEDIUM RISK - OUTBOUND TCP COMMUNICATION REQUIREMENTS NOT ALREADY PERMITTED.

-- HIGH RISK - TWO WAY IP/TCP/UDP COMMUNICATION REQUIREMENTS NOT ALREADY PERMITTED.

-- VERY HIGH RISK - UNACCEPTABLE PROTOCOLS OR REQUIREMENTS. MANDATORY KIOSK MITIGATION UNTIL DISCONTINUED OR REENGINEERED. THESE RISKS WILL BE CAPTURED BY THE ON-SITE IATT REPRESENTATIVES AND FORWARDED TO THE NMCI DAA IN THE VULNERABILITY ASSESSMENT LETTER. WHEN ALL CERTIFICATION TESTING RESULTS FOR A SITE ARE AVAILABLE TO THE NMCI DAA, HE WILL ISSUE A TYPE ACCREDITED BOUNDARY 2 FIREWALL POLICY FOR THE SITE AND ISSUE AN IATO COVERING THE SUITE OF APPLICATIONS AT THAT SITE. IN ADDITION TO THE VULNERABILITY ASSESSMENT RESULTS DISCUSSED ABOVE, THE IATO WILL CONSIDER THE STATE OF AVAILABLE SSAA DOCUMENTATION FOR EACH APPLICATION IN ACCORDANCE WITH THE FOLLOWING BOUNDARY 1 FIREWALL COMPLIANCE CATEGORIES:

- CATEGORY 1 - CLIENT APPLICATION IS NMCI CERTIFIED AND USES TRUSTED COMMUNICATIONS WITH THE SUPPORTING SERVER. EITHER THE SERVER APPLICATION OR BOTH CLIENT AND SERVER PORTIONS OF THE APPLICATION HAVE CERTIFICATION AND ACCREDITATION (C&A) PACKAGES AND CAN BE MOVED INTO NMCI TRUSTED ENCLAVE. SSAA PACKAGE IS COMPLETE AND THE APPLICATION IS ACCREDITED.

- CATEGORY 2 - CLIENT APPLICATION IS NMCI CERTIFIED, BUT CONCERNS EXIST ABOUT COMMUNICATIONS WITH THE SERVER BECAUSE OF A LACK OF COMPLETED DOCUMENTATION (NO DEPARTMENT OF DEFENSE (DOD) C&A.) SERVER APPLICATION IS NMCI CERTIFIED, BUT CONCERNS EXIST WITH THE SERVER'S COMMUNICATION WITH OTHER SERVERS AND/OR CLIENTS BECAUSE OF THE LACK OF COMPLETED DOCUMENTATION (NO DOD C&A.) NO BOUNDARY 2 MODIFICATIONS ARE REQUIRED. RISK IS MINIMIZED IF BOTH CLIENT AND SERVER ARE PLACED WITHIN NMCI ENCLAVE VICE LEAVING THE SERVER OUTSIDE THE NMCI ENCLAVE.

- CATEGORY 3 - CLIENT IS NMCI CERTIFIED, BUT SERVER HAS UNTRUSTED

COMMUNICATION REQUIREMENTS TO NON-NMCI USERS FOR THE RISK MITIGATION (ACCREDITATION) PHASE OR LONGER. SERVER APPLICATION IS NMCI CERTIFIED, BUT THE SERVER HAS UNTRUSTED COMMUNICATION REQUIREMENTS TO NON-NMCI SERVERS AND/OR USERS FOR THE RISK MITIGATION (ACCREDITATION PHASE OR LONGER. BOUNDARY 2 FIREWALL MODIFICATION IS REQUIRED.

- CATEGORY 4 - CLIENT APPLICATION MAY OR MAY NOT BE CERTIFIED, AND THERE IS UNTRUSTED COMMUNICATIONS BETWEEN CLIENT AND SERVER OR SERVER AND SERVER OR APPLICATION CLIENT/SERVER IS ACCESSIBLE TO THE GENERAL PUBLIC. NO DOD C&A SYSTEM CAN EITHER BE SUNSET-ED OR KIOSKED. A RULE SET GOVERNING SUPPORT FOR KIOSKED APPLICATIONS WILL BE PROVIDED SEPARATELY. BASED ON BOUNDARY 1 FIREWALL COMPLIANCE CATEGORY AND THE RISK LEVEL, THE NMCI DAA WILL ISSUE AN IATO REQUIRING SPECIFIC ACTIONS AND LIMIT THE AUTHORITY TO OPERATE FOR A SPECIFIED TIME PERIOD AS FOLLOWS:

CATEGORY 1 - LENGTH OF AUTHORITY TO OPERATE (ATO) (NORMALLY 3 YEARS).

CATEGORY 2 - ONE YEAR

CATEGORY 3 - SUBMIT PLAN OF ACTION MILESTONES (POA&M) FOR MIGRATION VIA APPLICABLE ECHELON II COMMAND WITHIN SIX MONTHS TO NAVY CIO FOR APPROVAL/DISAPPROVAL AND ANNUAL REVIEW.

CATEGORY 4 - POA&M SUBMITTED FOR MITIGATION/MIGRATION VIA APPLICABLE ECHELON II DUE WITHIN THREE MONTHS TO NAVY CIO. MIGRATION/TERMINATION MUST BE COMPLETED WITHIN NINE MONTHS.

E. RISK MITIGATION (ACCREDITATION): THE SECOND PHASE OF THE PROCESS COMMENCES AFTER NMCI SEAT CUTOVER AND INVOLVES THE COMPLETION OF THE RISK MITIGATION (ACCREDITATION) ERQ, FURTHER DEVELOPMENT OF RISK MITIGATION STRATEGIES, SUBMISSION OF POA&M FOR EACH APPLICABLE APPLICATION IAW IATO REQUIREMENTS, EXECUTION OF APPLICATION MITIGATION ACTION AND COMPLETION OF SSAA DOCUMENTATION. FAILURE TO COMPLETE REQUIRED MITIGATION ACTIONS (SUBMIT POA&M AND MEET TIMELINES) WILL RESULT IN EITHER DENIAL OF APPLICATION USE ON NMCI BY THE NAVY CIO OR POTENTIAL ADDITIONAL MITIGATION REQUIREMENTS. THE PRIMARY TASKS IN THIS PHASE ARE THE MITIGATIONS OF THE RISKS IDENTIFIED DURING THE CERTIFICATION PHASE AND THE COMPLETION OF THE SSAA DOCUMENTATION REQUIRED FOR CERTIFICATION. THERE HAVE BEEN MANY TECHNIQUES ALREADY DEVELOPED BY THE NMCI CONTRACTOR (INFORMATION STRIKE FORCE (ISF)) FOR CATEGORY 3 APPLICATIONS TO MITIGATE RISKS UNTIL THE SERVER CAN BE TRANSITIONED INTO THE NMCI ENCLAVE. COMPLETION OF RISK MITIGATION IS THE RESPONSIBILITY OF THE APPLICABLE ECHELON II COMMAND, INCLUDING APPLICABLE SUBORDINATE COMMANDS, THE CENTRAL DESIGN ACTIVITY (AS DESIGNATED IN PARAGRAPH 4.B) AND THE ISF. SSAA DOCUMENTATION IS SUBMITTED BY ECHELON II COMMAND OR CDA, AS APPROPRIATE, TO NMCI PROGRAM MANAGEMENT OFFICE (PMO) FOR INITIAL REVIEW AND EVALUATION PRIOR TO SUBMISSION TO THE NMCI DAA FOR APPROVAL. FOR CATEGORY 4 APPLICATIONS, A RECOMMENDATION TO MIGRATE OR TERMINATE THE APPLICATION WILL BE MADE AND APPROVED BY THE NAVY CIO. FOR ALL APPLICATIONS THAT ARE TO REMAIN IN THE NMCI, THE SSAA DOCUMENTATION WILL BE DEVELOPED BY THE ECHELON II COMMAND OR CDA, AS APPROPRIATE, AND SUBMITTED TO NMCI PMO FOR INITIAL REVIEW AND EVALUATION PRIOR TO SUBMISSION TO THE NMCI DAA FOR APPROVAL.

F. NAVY TRIAGE PROCESS: AN APPLICATION TRIAGE PROCESS, WHICH WILL BE DESIGNED TO REDUCE THE OVERALL NUMBER OF NAVY APPLICATIONS, WILL RUN CONCURRENTLY WITH NMCI CERTIFICATION AND THE RISK MITIGATION (ACCREDITATION) PHASES AT THE ECHELON II AND NAVY CIO LEVEL. THE PRODUCT OF THE NMCI CERTIFICATION PHASE, BOUNDARY 1 FIREWALL

COMPLIANCE CATEGORY AND RISK LEVEL, WILL BE USED TO ESTABLISH PRIORITIES AND IDENTIFY APPLICATIONS FOR ELIMINATION DURING THE TRIAGE PROCESS. THIS PROCESS WILL BE ADDRESSED SEPARATELY.

4. ACTION AND RESPONSIBILITIES. IN ORDER FOR THE MODIFIED PROCESS DEFINED IN PARAGRAPH 3 TO BE EFFECTIVE THE FOLLOWING SPECIFIC ACTION AND RESPONSIBILITIES ARE REQUIRED:
A. ECHELON II ARE RESPONSIBLE TO ENSURE THEY AND THEIR SUBORDINATE COMMANDS COMPLY WITH THE FOLLOWING:
(1) 60 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND DELIVERS THE COMPLETED LIST OF ALL COTS AND GOTS APPLICATIONS REQUIRED TO OPERATE ON NMCI AND RATIONALIZED BY THEIR ECHELON II COMMAND. 50 PERCENT OF ALL GOTS APPLICATIONS MUST BE DELIVERED AND ACCEPTED BY THE ISF FOR CERTIFICATION.
(2) 45 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND SHALL HAVE 75 PERCENT OF IDENTIFIED APPLICATIONS (COTS AND GOTS) DELIVERED AND ACCEPTED FOR CERTIFICATION.
(3) 30 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND SHALL ENSURE ALL REMAINING IDENTIFIED APPLICATIONS (COTS AND GOTS) MUST BE SUBMITTED AND ACCEPTED FOR CERTIFICATION. APPLICATIONS NOT SUBMITTED BY THIS DEADLINE WILL NOT TRANSITION TO NMCI ON THE SCHEDULED CUTOVER DATE.
(4) 14 DAYS PRIOR TO START OF CUTOVER, ALL APPLICATIONS REQUIRED FOR CUTOVER ARE CERTIFIED.
(5) ALL INCREMENT 1.0 COMMANDS MUST HAVE COMPLETED SUBMISSION OF THEIR FINALIZED RATIONALIZED APPLICATION LIST TO NMCI PMO. THE APPROPRIATE ECHELON II COMMAND SHOULD HAVE PREVIOUSLY APPROVED THIS RATIONALIZED LIST OR DO SO NLT 21 MARCH 2002.
(6) ALL INCREMENT 1.5 COMMANDS MUST HAVE THEIR RATIONALIZED LIST OF APPLICATIONS SUBMITTED VIA THEIR APPLICABLE ECHELON II COMMAND NLT 21 MARCH 2002.
(7) APPLICATIONS SHALL BE SUBMITTED AS NOTED ABOVE USING THE REQUEST FOR SERVICE (RFS) AND CERTIFICATION PHASE ERQ. ALL DATA ELEMENTS IDENTIFIED IN THE RFS AND IN THE CERTIFICATION PHASE AND THE RISK MITIGATION (ACCREDITATION) PHASE ERQ ARE MANDATORY IN ORDER FOR THIS SUBMISSION TO BE CONSIDERED COMPLETE.
B. DESIGNATION OF CDA: CRITICAL TO THE LEGACY APPLICATION PROCESS IS THE ASSIGNMENT OF RESPONSIBILITY FOR EVERY APPLICATION TO BE CERTIFIED OR ACCREDITED. THIS MESSAGE ASSIGNS RESPONSIBILITIES TO CENTRAL DESIGN ACTIVITIES (CDA) AND DETAILS THE PROCESS TO ASSIGN CDA RESPONSIBILITIES WHEN A DESIGNATED CDA DOES NOT EXIST. IN ORDER TO EXPEDITE THE CERTIFICATION AND ACCREDITATION PROCESS, CDA(S) FOR APPLICATIONS WHICH EXIST AT MORE THAN ONE SITE, SHALL SUBMIT SSAA DOCUMENTATION FOR THE APPLICABLE APPLICATION ONCE VICE REQUIRING DUPLICATION OF CDA RESPONSIBILITIES AT MULTIPLE SITES BY MULTIPLE ECHELON II COMMANDS. CDA HAS PRINCIPAL RESPONSIBILITY FOR DESIGN, DEVELOPMENT, DOCUMENTATION, AND LIFE CYCLE MAINTENANCE OF APPLICATIONS, INCLUDING INITIAL PRODUCT DELIVERY AND DISTRIBUTION OF UPDATES. ADDITIONALLY, CDA(S) RESOURCE AND MAINTAIN HELP DESK SERVICES FOR THEIR APPLICATIONS. THE PRIMARY DON CDA(S) ARE CONTROLLED BY NAVSEA, NAVAIR, SPAWAR, NAVSUP, NAVFAC, CNET, MARINE CORPS SYSTEMS COMMAND AND DISTRIBUTED TO SOME OF THEIR SUBORDINATE COMMANDS (E.G. NAVSUP HAS FLEET MATERIALS SUPPORT OFFICE (FMSO) PROVIDE THEIR CDA RESPONSIBILITIES). THE FOLLOWING CATEGORIES OF APPLICATIONS AND THEIR ASSOCIATED CDA IDENTIFICATION AND DESIGNATION RESPONSIBILITY ARE ASSIGNED:
(1) NAVY SYSTEM COMMAND DEVELOPED GOTS - APPLICABLE SYSCOM IS RESPONSIBLE FOR IDENTIFICATION, DESIGNATION OF THE CDA AND ENSURING

SUBSEQUENT CDA RESPONSIBILITIES ARE ACCOMPLISHED IAW THIS MESSAGE.
(2) MARINE CORPS SYSTEM COMMAND DEVELOPED GOTS - APPLICABLE NAVY ECHELON II IS RESPONSIBLE FOR REPORTING THE APPLICATION ASSOCIATED SYSCOM TO NAVY CIO, MARINE CORPS CIO OFFICE AND NMCI PMO. THE NAVY CIO WILL WORK WITH MARINE CORPS CIO OFFICE AND NMCI PMO FOR CDA IDENTIFICATION, DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(3) INDIVIDUAL COMMAND DEVELOPED GOTS - APPLICABLE ECHELON II IS RESPONSIBLE FOR IDENTIFICATION, DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(4) OTHER SERVICE/JOINT/OSD AND OTHER AGENCY DEVELOPED GOTS - APPLICABLE ECHELON II IS RESPONSIBLE FOR IDENTIFICATION OF THE APPLICATION AND ITS SOURCE TO NAVY CIO AND NMCI PMO. THE NAVY CIO WILL WORK WITH DON CIO AND NMCI PMO FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(5) NON-GOVERNMENT, NON-COMMERCIAL PRODUCTS - APPLICABLE ECHELON II WHOSE SUBORDINATE COMMAND PURCHASED THE PRODUCT FOR USE IS RESPONSIBLE FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(6) COMMERCIAL PRODUCTS (COTS) - APPLICABLE ECHELON II WHOSE SUBORDINATE COMMAND PURCHASED THE PRODUCT FOR USE IS RESPONSIBLE FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION. FOR APPLICATIONS CONTAINED IN THE NMCI BASIC DESKTOP SEAT, IDENTIFICATION AND DESIGNATION OF CDA IS NOT REQUIRED. IN THE FUTURE, AS ENTERPRISE APPLICATIONS ARE DESIGNATED AND CENTRALLY PURCHASED CDA RESPONSIBILITIES WILL BE ASSIGNED TO THE VENDOR AND INCLUDED IN THE ACQUISITION AGREEMENT.
C. ECHELON II AND CDA RESPONSIBILITIES: AS APPLICABLE, EACH ECHELON II COMMAND IS RESPONSIBLE FOR ENSURING THEIR CDA(S) SUBMIT THE APPLICATION SSAA DOCUMENTATION TO NMCI PMO. FOR EXAMPLE, THE CDA FOR THE NAVAL AIR LOGISTICS COMMAND MANAGEMENT INFORMATION SYSTEM (NALCOMIS) IS SPAWAR SO SPAWAR SHOULD ENSURE THE CDA FOR NALCOMIS COMPLIES WITH THE REQUIREMENTS OF THIS MESSAGE. AS A JOINT EXAMPLE, THE CDA FOR THE DEFENSE MESSAGE SYSTEM (DMS) IS DISA, SO ECHELON II REPORTS THE SOURCE OF DMS AS DISA AND THE NAVY CIO WILL WORK WITH DON CIO TO ENSURE DISA HAS THEIR DMS CDA COMPLY WITH THE REQUIREMENTS OF THIS MESSAGE. THESE KNOWN CDA(S) SHOULD BE PROVIDING THE REQUIRED SSAA DOCUMENTATION AND THE NMCI PMO WILL CONDUCT AN INITIAL REVIEW OF THE SSAA FOR CONSIDERATION AS ADEQUATE DOCUMENTATION FOR ALL NMCI COMMAND AND SITE IMPLEMENTATIONS. THIS CDA SUBMITTED SSAA DOCUMENTATION WILL BE EVALUATED AND ASSIGNED THE FOLLOWING STATUS: (A) SATISFACTORY AS A SSAA FOR NMCI, OR (B) NOT SATISFACTORY AS A SSAA FOR NMCI BUT DOES INCLUDE THE NECESSARY INFORMATION FOR COMPLETION OF THE NMCI CERTIFICATION PROCESS, OR (C) INCOMPLETE. SATISFACTORY SSAA'S WILL BE SUBMITTED TO THE NMCI CERTIFICATION AND ACCREDITATION REVIEW PANEL (NCARP) FOR ENTERPRISE ACCREDITATION. IF THIS CDA SUBMITTED SSAA DOCUMENTATION IS NOT A SATISFACTORY SSAA FOR NMCI OR IS INCOMPLETE, NMCI PMO WILL REPORT THIS TO THE NMCI DAA, THE LOCAL DAA(S) AND CAUSE A FORMAL MESSAGE TO BE PREPARED TASKING THE APPLICABLE CDA TO TAKE ACTION TO ENSURE MINIMUM REQUIREMENTS FOR SEAT CUTOVER ARE COMPLETED IMMEDIATELY. THE CDA MUST ENSURE SUBSEQUENT SSAA DOCUMENTATION IS COMPLETED IN ACCORDANCE WITH THE IATO TIME REQUIREMENTS FOR THE SPECIFIC APPLICATION. THE FOLLOWING SPECIFIC ACTION AND RESPONSIBILITIES NEED TO BE FOLLOWED BY THE CDA(S):
- MUST HAVE COMPLETED SUBMISSION OF AN RFS FOR EACH APPLICATION NLT 21 MARCH 2002 USING THE NMCI APPLICATION DATABASE. (THE 21

MARCH 2002 DATE DOES NOT APPLY TO AN APPLICATION WHICH NEVER HAD A DESIGNATED CDA. FOR THESE APPLICATIONS, THE NEWLY DESIGNATED CDA SHOULD PROVIDE THE RFS DOCUMENTATION NLT 11 MAY 2002.)
- MUST HAVE COMPLETED SUBMISSION OF ALL CLIENT MEDIA TO THE ISF NLT 21 APRIL 2002. (THE 21 APRIL 2002 DATE DOES NOT APPLY TO AN APPLICATION WHICH NEVER HAD A DESIGNATED CDA. FOR THESE APPLICATIONS, THE NEWLY DESIGNATED CDA SHOULD PROVIDE THE CLIENT MEDIA NLT 11 MAY 2002.)
- FOR SUBSEQUENT UPGRADES/PATCHES TO EXISTING APPLICATIONS, MUST SUBMIT AN RFS USING THE NMCI APPLICATION DATABASE AND SUBMIT MEDIA TO THE ISF FOR CERTIFICATION. EACH CDA IS RESPONSIBLE FOR INDEPENDENT CERTIFICATION AND ACCREDITATION OF ANY CHANGES TO THEIR APPLICATIONS AS DESIGNATED BY THE NMCI DAA. FURTHER DETAILS ON A NMCI FOLLOW-ON CERTIFICATION AND ACCREDITATION PROCESS ARE BEING DEVELOPED AND WILL BE PROVIDED SEPARATELY.
- MUST CHANGE APPLICATION DISTRIBUTION AND NOTIFICATION PROCESSES. FOR AN INTERIM PERIOD, THEY MUST DEVELOP PARALLEL PROCESSES FOR NMCI AND NON-NMCI SITES. FOR NMCI SITES, APPLICATIONS MUST NOT BE DELIVERED TO SITES WITHOUT FIRST UNDERGOING NMCI CERTIFICATION AND ACCREDITATION.
- MUST STANDARDIZE APPLICATIONS TO REDUCE MULTIPLE VERSIONS. IMPLEMENTATION OF APPLICATIONS ON NMCI SHOULD GREATLY FACILITATE THESE EFFORTS.
- MUST ENSURE DESIGNATED HELP DESK SUPPORT ACTIVITIES ARE WORKING SEAMLESSLY WITH NMCI HELP DESKS. WORKING GROUPS ARE IN THE PROCESS OF DEFINING NMCI AND LEGACY SYSTEM HELP DESK PROCESSES. EACH CDA WILL BE CONTACTED TO PARTICIPATE.
- MUST COMPLETE REQUIRED SSAA DOCUMENTATION FOR ALL APPLICATIONS INTENDED FOR CONTINUED USE ON NMCI. FOR INCREMENT 1.0 AND 1.5 SITES, THE SSAA DOCUMENT IS REQUIRED BY 01 AUGUST 2002. FOR ALL OTHER APPLICATIONS, THE SSAA IS REQUIRED NLT 01 SEPTEMBER 2002.
D. REPORTING: THE PRIMARY TOOL TO ENSURE ACCURATE REPORTING OF LEGACY APPLICATIONS STATUS IS THE NMCI DATABASE. EACH ECHELON II COMMAND WILL TAKE APPROPRIATE ACTION TO ENSURE ALL DATA ELEMENT ENTRIES ARE COMPLETE, ACCURATE, AND MAINTAINED CURRENT FOR THEIR COMMAND AND SUBORDINATE COMMANDS. THIS INCLUDES THE IDENTIFICATION OF EACH APPLICATION'S CDA. THE NMCI PMO WILL CONSOLIDATE THIS DATA FOR WEEKLY REPORTING TO SECNAV AND CNO. REPORTS WILL REFLECT STATUS OF RATIONALIZATION, RFS SUBMISSION, CERTIFICATIONS, ACTION PLANS, AND SSAA DOCUMENTATION.

5. SPECIFIC NAVY POLICY, GUIDANCE AND GOALS WILL BE PROVIDED SHORTLY CONCERNING THE FURTHER REDUCTION OF LEGACY APPLICATIONS AND THE ELIMINATION OF LEGACY NETWORKS REQUIRED TO SUPPORT KIOSKED APPLICATIONS.

6. THIS PROCESS MODIFICATION IS REQUIRED TO FACILITATE THE IMPLEMENTATION AND COMPLETION OF NMCI WITHIN DON. YOUR PERSONAL ATTENTION AND SUPPORT IS REQUESTED TO ENSURE SUCCESS.

7. RELEASED BY VADM R. W. MAYO, USN.//

BT
NNNN

D2. Navy CNO Message R 301245Z SEP 02

R 301245Z SEP 02 CNO WASHINGTON DC ENTERPRISE STRATEGY FOR MANAGING NMCI APPLICATIONS AND DATABASES
ADMINISTRATIVE MESSAGE
ROUTINE
UNCLAS
MSGID/GENADMIN/CNO WASHINGTON DC N6N7/006-02//
SUBJ/ENTERPRISE STRATEGY FOR MANAGING NMCI APPLICATIONS AND DATABASES //
REF/A/GENADMIN/CNO WSHINGTON DC/252250ZFEB2002/001-02//
NARR/REF A IS NAVY INFORMATION OFFICER MESSAGE DIRECTING ECHELON II COMMANDERS TO IMPLEMENT PROCESSES TO REDUCE APPLICATIONS AND DATABASES WITHIN THEIR COMMANDS USING THE ISF TOOLS DATABASE.// POC/TRAVERSO, TIMOTHY/-/CNO NIO/-/TEL:703-604-7806//
AMPN/EMAIL: TRAVERSO.TIMOTHY@HQ.NAVY.MIL//
POC/STICINSKI, RON/CAPT/NADTF/-/TEL:202-764-2942//
AMPN/EMAIL: RON.STICINSKI@NAVY.MIL//
POC/CORMAN, CYNTHIA/-/NADTF/-/TEL:202-764-0852//
AMPN/EMAIL: CYNTHIA.CORMAN@NAVY.MIL//
POC/HEDIN, TED/-/NADTF/-/TEL:202-764-0012//
AMPN/EMAIL: HEDINW@NCTC.NAVY.MIL//
POC/KELLY, JUDY/LCDR/NADTF/-/TEL:202-764-1813//
AMPN/EMAIL: JUDY.KELLY@NAVY.MIL//
RMKS/1. THIS IS A COMBINED DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO), NAVY INFORMATION OFFICER (NIO) AND DIRECTOR, NMCI MESSAGE.
2. THE REDUCTION AND CONSOLIDATION OF NAVY APPLICATIONS AND DATABASES TO THE ABSOLUTE MINIMUM REQUIRED TO SUPPORT THE NAVY'S MISSION IS THE PRIMARY GOAL. COORDINATING THE EFFORTS OF FUNCTIONAL AREA MANAGERS (FAMS), ECHELON II COMMANDS, NAVY APPLICATION AND DATABASE TASK FORCE (NADTF), NETWARCOM (NMCI DESIGNATED APPROVAL AUTHORITY (DAA)), TASK FORCE WEB (TFW), AND THE ENTERPRISE RESOURCE PLANNING (ERP) PILOTS, WITHOUT IMPACTING NMCI SEAT ROLLOUT, REQUIRES A COMMON OPERATIONAL PICTURE OF THE NAVY'S APPLICATIONS AND DATABASES. CURRENTLY THE FOLLOWING CONDITIONS EXIST: A. THE ISF TOOLS DATABASE IS THE AUTHORITATIVE DATABASE FOR NAVY APPLICATIONS ON NMCI AND IT IS THE TOOL FOR EVERY NAVY COMMAND TO ENSURE OPERATIONALLY REQUIRED APPLICATIONS ARE ORDERED FOR NMCI IMPLEMENTATION. B. THE DEPARTMENT OF THE NAVY (DON) APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS) HAS ACHIEVED INITIAL OPERATIONAL CAPABILITY. DADMS WILL BE THE SINGLE AUTHORITATIVE DATABASE FOR ALL APPLICATIONS AND DATABASES, WILL CONTAIN A COMPLETE INVENTORY OF ALL AUTHORIZED APPLICATIONS AND DATABASES RESIDING ON ALL NAVY NETWORKS (E.G. NMCI, IT21 AND OCONUS BLII) AND WILL SERVE AS A TOOL TO IDENTIFY AND TRACK QUARANTINED APPLICATIONS. THIS MESSAGE DIRECTS ACTION TO ACHIEVE COMMON OPERATIONAL PICTURE OF THE NAVY'S APPLICATIONS AND DATABASES IN DADMS AND THE CONTINUED USE OF THE ISF TOOLS DATABASE AS THE PRIMARY TOOL FOR ORDERING AND IMPLEMENTING APPLICATIONS IN NMCI. THIS MESSAGE DIRECTS ALL ECHELON II COMMANDS TO ENSURE THEIR FINAL RATIONALIZED LIST OF ALL NMCI APPLICATIONS (AT HEADQUARTERS AND ALL SUBORDINATE COMMANDS) IS REFLECTED IN THE ISF TOOLS DATABASE WITHIN SIXTY DAYS OF THE DATE TIME GROUP OF THIS MESSAGE, REQUIRES THE APPROVAL OF THE APPLICABLE FAM AND NIO FOR THE SUBSEQUENT ADDITION OF APPLICATIONS TO ISF TOOLS DATABASE BY ECHELON II COMMANDS AND SUBORDINATE COMMANDS, MANDATES THAT EVERY NAVY APPLICATION WILL HAVE A DESIGNATED CENTRAL DESIGN ACTIVITY AND/OR OWNER IDENTIFIED BY NAME WITH CONTACT INFORMATION IAW PARA 4 OF REF A, AND SPECIFIES A PROCESS TO BE FOLLOWED TO TRACK ALL QUARANTINED APPLICATIONS.

3. REQUIRED ACTION AND THE ASSOCIATED TIME LINE IS POSTED
AT HTTPS:"FWD DOUBLE SLASH"WWW.DADMS.NAVY.MIL UNDER THE "POLICY AND
GUIDANCE" LINK.//
BT
#0179
NNNN

D3. Navy CNO Message COSPAWARSYSCOM/PMW164 242225Z MAY 02

Prec: ROUTINE
DTG: 242225Z MAY 02
Subj: NMCI PROCESS SUMMIT AGREEMENTS//

UNCLAS //N2060//

MSGID/GENADMIN/COMSPAWARSYSCOM/PMW164//

SUBJ/NMCI PROCESS SUMMIT AGREEMENTS//

REF/A/GENADMIN/PEO IT WASHINGTON DC/202304ZMAY2002//

AMPN/REF A IS NMCI 20K ROLLOUT EXECUTION ORDER.//
POC/ROBERT LOGAN/COL/NMCI DEPUTY DIRECTOR/-/TEL:CML:(703)685-5510
/EMAIL:RLOGAN'AT'SPAWAR.NAVY.MIL//
POC/CRAIG MADSEN/CAPT/NAVY NMCI PM/-/TEL:(619)524-7553
/EMAIL:EMAIL: MADSENC'AT'SPAWAR.NAVY.MIL//
POC/RICH GLOVER/CIV/PM USMC NMCI/-/TEL:DSN:278-0709
/EMAIL:EMAIL: GOVERRA'AT'MCSC.USMC.MIL//
POC/TIM TRAVERSO/CIV/NADTF-NAVY CIO/-/TEL:(703)602-5995
/EMAIL:EMAIL: TRAVERSO.TIMOTHY'AT'HQ.NAVY.MIL//

RMKS/1. THIS IS A COORDINATED NAVAL MESSAGE FROM DIRECTOR NMCI, NAVY AND MARINE CORPS PROGRAM OFFICES, AND THE NMCI ISF. ON MAY 7 - 9, REPRESENTATIVES FROM THESE ORGANIZATIONS HELD A SUMMIT TO DISCUSSAND DEFINE PROCESSES TO IMPROVE AND ACCELERATE NEAR TERM NMCI SEATROLLOUT. THIS NAVAL MESSAGE SUMMARIZES THE AGREEMENTS REACHED ON THESE PROCESSES.

2. BACKGROUND. FUTURE NMCI CUSTOMERS HAVE SEEN A VARIETY OF PROCESS DOCUMENTS, HAVE ATTENDED VARIOUS NMCI FORUMS, OR HAVE HAD THE OPPORTUNITY TO OBSERVE THE EARLY NMCI INSTALLATION EFFORTS. TO DATE, NMCI SEAT ROLLOUT HAS BEEN SLOWER THAN EXPECTED OR DESIRED. THROUGH A COMBINED EFFORT AT THE NMCI PROCESS SUMMIT, HIGH LEVERAGE ITEMS WERE IDENTIFIED RELATED TO LEGACY APPLICATIONS AND INFORMATION ASSURANCE. ALSO, RELATED NMCI TRANSITION ISSUES WERE IDENTIFIED AND PRIORITIZED.

3. PROCESS CHANGES. THE DIRECTOR NMCI AUTHORIZES THE PROCESSES SUMMARIZED BELOW FOR IMMEDIATE IMPLEMENTATION AT SITES TRANSITIONING TO NMCI IN ACCORDANCE WITH REF A. SPECIFIC PROCESS DETAILS WILL BE PROVIDED SEPCOR, BUT THE SIGNIFICANT CHANGES ARE SUMMARIZED BELOW.
A. LEGACY APPLICATIONS:
(1) LOCAL APPLICATION LOADING (EITHER MANUALLY OR THROUGH AN IMAGE BUILD) IS APPROVED. APPLICATIONS SUITABLE FOR LOCAL LOADING MUST BE ON THE SITE'S RATIONALIZED LIST.
(2) USER TO APPLICATION MAPPING WILL BE REQUIRED AT THE TIME FINAL RATIONALIZED LISTS ARE DUE (AOR-60 DAYS).
(3) REVISE LEGACY APPLICATION PROCESSES TO SHORTEN TIMELINE BY APPLYING APPLICATION "FUNNELING" PROCESSES AND EMPOWERING THE NADTF TO APPLY APPLICATION RULE SETS TO REDUCE RATIONALIZED LISTS.
ON-SITE LEADERSHIP WILL EXPLAIN THE FUNNELING PROCESS IN DETAIL.
ITS PURPOSE IS TO QUICKLY SORT AND PRIORITIZE EXISTING LEGACY APPLICATIONS.
(4) THE LEGACY APPLICATION MIGRATION RULE SET (LED BY NADTF)

INCLUDES THE FOLLOWING:
(A) WINDOWS 2000 COMPLIANT APPLICATIONS ONLY
(B) COMPLIANT WITH DON/DOD SECURITY POLICY
(C) NO PERSONAL, NON-MISSION, OR NON-BUSINESS-RELATED SOFTWARE
(D) NO GAMES
(E) NO FREEWARE OR SHAREWARE
(F) NO BETA OR TEST VERSION SOFTWARE PACKAGES
(G) NO APPLICATION DEVELOPMENT SOFTWARE (EXCEPTION APPLIES FOR APPROVED SCIENCE AND TECHNOLOGY [S&T] SEATS)
(H) NO AGENTS
(I) NO DUPLICATION OF STANDARD SEAT SERVICES
(J) NO 8 OR 16 BIT APPLICATIONS
(5) ALL MEDIA NEEDS TO BE HELD ONSITE AND SUBMITTED TO THE ISF. CONTINUE TO USE THE ISF TOOLS DB TO CREATE REQUEST FOR SERVICE (RFS) FOR ALL LEGACY APPLICATIONS REQUIREMENTS.
(6) IA VULNERABILITY ASSESSMENT PACKAGES WILL BE DEVELOPED AND PROVIDED POST SEAT CUTOVER VICE PRIOR TO SEAT CUTOVER.
(7) APPLICATIONS WILL BE TESTED USING A PIAB, A LADRA TEST SEAT, OR THE ISF CERTIFICATION LAB IN SAN DIEGO. ISF WILL DETERMINE MEANS AND LOCATION OF TESTING.
(8)APPLICATIONS THAT SUCCESSFULLY PASS NMCI CERTIFICATION AND B1/B2 TESTING WILL BE AUTHORIZED FOR OPERATION ON NMCI.
(9)ISF WILL GENERATE A WEEKLY REPORT FOR DELIVERY TO THE NMCI DAA. THE WEEKLY REPORT WILL PROVIDE INFORMATION PERTAINING TO APPLICATION INSTALLATION METHOD, TESTING RESULTS, AND NUMBER OF SEATS INSTALLED FOR EACH SITE.
(10) APPLICATIONS THAT FAIL CERTIFICATION AND/OR B1/B2 TESTING WILL BE QUARANTINED ON THE LEGACY NETWORK.
(11) APPLICATIONS THAT ARE IDENTIFIED, SUBMITTED, OR APPROVED LATE WILL BE QUARANTINED ON THE LEGACY NETWORK.
B. INFORMATION ASSURANCE: THE FOLLOWING ISSUES HAVE RECEIVED PROGRAM ENDORSEMENT AND HAVE BEEN FORWARDED TO THE NMCI DAA FOR APPROVAL.
(1) SHORTEN TIMELINE TO ACHIEVE SITE IATO FROM 31 DAYS TO 24 DAYS INCLUDING 8 DAYS FOR FORMAL DAA REVIEW AND APPROVAL. DAA TO ASSIGN DELEGATE AUTHORITY TO ASSIST IN OVERCOMING DAA AVAILABILITY. ISF/PMO TO PROVIDE DAA 24-72 HOUR NOTICE OF UPCOMING CRITICAL DECISION MILESTONES.
(2) IATO/IATC IN PARALLEL. GOVERNMENT APPROVAL TO LAUNCH APPLICATIONS TO TEST SEATS ON THE OPERATIONAL NETWORK FOR TESTING. APPROVAL EXTENDS TO APPLICATIONS AND SEATS USED FOR NMCI SECURITY/GPO TESTING ONLY. APPLICATIONS INCLUDE ONLY THOSE CURRENTLY RUNNING IN LEGACY ENVIRONMENT.
(3) ON COMPLETION OF BOUNDARY 2 BUILD AND SCAN, DAA TO APPROVE, IN PHONECON OR EMAIL VICE LETTER, CONNECTION TO NETWORK.
(4) ON COMPLETION OF SERVER FARM BUILD AND SCAN, DAA TO APPROVE, IN PHONE CON OR EMAIL VICE LETTER, APPROVAL TO CONNECT TO BOUNDARY.

4. WORKING ISSUES. IN ADDITION TO THE LEGACY APPLICATION AND INFORMATION ASSURANCE PROCESS CHANGES OUTLINED ABOVE, WORK CONTINUES ON COMMAND AND CONTROL AT SITES, THE ROLLOUT SCHEDULE BEYOND THE FIRST 20K SEATS, AN ENTERPRISE POLICY/PLAN TO BASELINE THE KIOSK PROCESS, AND THE USER TO APP MAPPING PROCESS. APPROXIMATELY 50 TRANSITION ISSUES WERE IDENTIFIED AS HAVING THE POTENTIAL TO DIRECTLY EFFECT RAPID SEAT ROLLOUT AND WILL ALSO CONTINUE TO BE WORKED. EXAMPLES OF THESE ISSUES INCLUDE MACS, S&T CLIN 0038, LEGACY DEVICE SUPPORT, AND END USER AVAILABILITY.

5. THE NMCI DIRECTOR'S OFFICE, NAVY AND MARINE CORPS PROGRAM OFFICES, AND THE ISF WILL CONTINUE TO REFINE PROCESSES TO INCORPORATE LESSONS LEARNED AS SEAT ROLLOUT CONTINUES. YOUR CONTINUED INVOLVEMENT AND COMMENTS ARE BOTH SPECIFICALLY REQUESTED AND APPRECIATED.//

BT
#5456
NNNN

D4. Navy CNO 120155Z JUN 02

120155Z JUN 02 CNO WASHINGTON DC NAVY STANDARD APPLICATIONS//

ADMINISTRATIVE MESSAGE
ROUTINE
UNCLAS
4630
MSGID/GENADMIN/CNO N09T/005-02//

SUBJ/NAVY STANDARD APPLICATIONS//

REF/A/MSG/CNO WASHINGTON DC/012017ZMAR2002//

REF/B/MSG/CNO WASHINGTON DC/252250ZFEB2002//

NARR/REF A IS NAVY INFORMATION OFFICER MESSAGE (CNO N09T 002-02) ESTABLISHING STANDARD APPLICATIONS TO BE USED ON NAVY NETWORKS. REF B IS NAVY INFORMATION OFFICER MESSAGE (CNO N09T 001-02) ON NMCI LEGACY APPLICATIONS TRANSITION PROCESS.//
POC/ALAND, DAVID/CAPT/CNO OPNAV N6K/LOC:WASHINGTON DC.
/EMAIL:(703) 604-6880 ALAND.DAVID(AT)HQ.NAVY.MIL//

RMKS/1. THIS MESSAGE IS A JOINT NAVY INFORMATION OFFICER AND DIRECTOR NMCI MESSAGE AND DIRECTLY SUPPORTS THE IMPLEMENTATION OF NMCI, INTEROPERABILITY BETWEEN NAVY NETWORKS AND USERS AND STANDARDIZATION OF COMMERCIAL OFF THE SHELF (COTS) AND GOVERNMENT OFF THE SHELF (GOTS) APPLICATIONS IN THE NAVY.

2. THIS MESSAGE CANCELS REF A AND PROVIDES ADDITIONAL MANDATORY DIRECTION FOR COTS APPLICATION REDUCTION THAT SHOULD BE APPLIED IMMEDIATELY TO ALL NAVY NETWORKS (E.G. NMCI, IT21 AND OCONUS BLII). SPECIFICALLY, THE APPLICATIONS AND ASSOCIATED VERSIONS LISTED IN PARAGRAPHS 3.A AND 4.A BELOW REPRESENT THE NAVY'S PREFERRED APPLICATIONS FOR ALL NAVY NETWORKS BASED UPON WIDE SPREAD USE THROUGH-OUT THE NAVY AND/OR OPERATIONAL REQUIREMENTS AS SPECIFIED BY FUNCTIONAL AREA MANAGERS. SOME NAVY NETWORKS MAY REQUIRE DIFFERENT COTS APPLICATIONS THAT PERFORM THE SAME OR SIMILAR FUNCTIONS OR A DIFFERENT VERSION OF THE APPLICATION LISTED. FOR THOSE COTS APPLICATIONS, FOLLOW THE EXCEPTION GUIDANCE LISTED BELOW IN
PARAGRAPH 3.B OR 4.C. AS TECHNOLOGY ADVANCES AND APPLICATIONS ARE REVISED, THE NMCI PROVIDED BASIC SEAT SERVICES (PARAGRAPH 3.A) AND THE OTHER COTS AND GOTS APPLICATIONS (PARAGRAPH 4.A) WILL BE UPDATED TO REFLECT THOSE ADVANCES AND REVISIONS AS SPECIFIED BY THE APPLICABLE FUNCTIONAL AREA MANAGER.

3. EACH ECHELON II COMMAND SHALL ESTABLISH APPLICATION AND APPLICATION VERSION CONTROL AS SOON AS POSSIBLE ON THE FOLLOWING STANDARDIZED APPLICATIONS BEING PROVIDED AS NMCI BASIC SEAT SERVICES FOR THE INDICATED COTS APPLICATIONS. UNLESS OTHERWISE APPROVED BY THE NAVY INFORMATION OFFICER, ECHELON II COMMANDS WILL ELIMINATE ANY UNNECESSARILY DUPLICATIVE APPLICATION FROM THEIR RATIONALIZED LIST:
A. COTS FUNCTION APPLICATION/VERSION
OPERATING SUITE MICROSOFT WINDOWS 2000 BUILD 2195 SP1
OFFICE SUITE MICROSOFT OFFICE PRO 2000 SR-1A
WORD PROCESSING MICROSOFT WORD 2000 9.0.3821 SR1
DESKTOP DATABASE MICROSOFT ACCESS 2000 9.0.3821 SR-1

PRESENTATIONS MICROSOFT POWER POINT 2000 9.0.5519
SPREADSHEETS MICROSOFT EXCEL 2000 9.0.3821 SR1
EMAIL CLIENT MICROSOFT OUTLOOK 2000 9.0.0.3821
CALENDAR MICROSOFT OUTLOOK 2000 9.0.0.3821
INTERNET BROWSER MICROSOFT INTERNET EXPLORER 5.5 SP-1 128 BIT
INTERNET BROWSER COMMUNICATOR 4.76 (NETSCAPE)
VIRUS PROTECTION NORTON A/V CORP EDITION V7.51 (SYMANTEC)
PDF VIEWER ACROBAT READER V.4.05D (ADOBE)
TERMINAL EMULATOR REFLECTION 8.0.5 (WRQ) HOST (TN3270,VT100, X-TERMINAL)
COMPRESSION TOOL WINZIP V.8 (WINZIP)
COLLABORATION TOOL NET MEETING V3.01 (4.4.3385)
MULTIMEDIA REAL PLAYER 8 (REAL NETWORKS)
MULTIMEDIA WINDOWS MEDIA PLAYER V7.0.0.1956
WEB CONTROLS MACROMEDIA SHOCKWAVE V 8.0 (MACROMEDIA)
WEB CONTROLS FLASH PLAYER 5.0 (MACROMEDIA)
WEB CONTROLS APPLE QUICKTIME MOVIE AND AUDIO VIEWER V4.12 (APPLE)
WEB CONTROLS IPIX V6.2.0.5 (INTERNET PICTURES)
SECURITY INTRUDER ALERT V3.6 (AXTENT)
SECURITY ESM V5.1 (AXTENT)
SOFTWARE MGMT RADIA CLIENT CONNECT (NOVADIGM)
INVENTORY, REMOTE CONTROL TIVOLI TMA 3.7 (IBM/TIVOLI)
DIAL-UP CONNECTIVITY PAL (MCI/WORLDCOM)
VPN VPN CLIENT (ALCATEL)
B. IF AN ECHELON II COMMANDER REQUIRES AN ADDITIONAL VERSION OF A COTS APPLICATION PROVIDED BY NMCI BASIC SEAT SERVICES (PARAGRAPH 3.A) OR OTHER COTS APPLICATIONS PERFORMING THE SAME FUNCTION, THE ECHELON II COMMANDER MUST REQUEST AN EXCEPTION SEPARATELY FROM BOTH THE NAVY INFORMATION OFFICER AND THE APPLICABLE FUNCTIONAL AREA MANAGER. ANY EXCEPTION REQUEST SHOULD INCLUDE THE NUMBER OF LICENSES HELD FOR EACH VERSION, THE NUMBER OF ACTUAL USERS OF EACH VERSION, THE PLAN FOR MIGRATING TO THE CORRESPONDING APPLICATION PROVIDED BY THE NMCI BASIC SEAT SERVICES AND JUSTIFICATION FOR INCLUDING THE APPLICATION FOR TRANSITION TO NMCI, OR RETAINING THE APPLICATION FOR USE ON IT21 OR OCONUS BLII NETWORKS (INCLUDE THE UNIQUE FUNCTION BEING PERFORMED BY THIS OTHER APPLICATION AND WHY IT IS OPERATIONALLY REQUIRED).

4. EACH ECHELON II COMMAND SHALL ESTABLISH APPLICATION AND APPLICATION VERSION CONTROL AS SOON AS POSSIBLE ON THE FOLLOWING ADDITIONAL STANDARDIZED COTS AND GOTS APPLICATIONS. ECHELON II COMMANDS WILL UPDATE APPLICATION VERSIONS ON THEIR RATIONALIZED LIST IN THE INFORMATION STRIKE FORCE (ISF) TOOLS DATABASE TO REFLECT THE VERSIONS LISTED BELOW:
A. SOFTWARE FUNCTION APPLICATION/VERSION
ALCOHOL AND DRUG MANAGEMENT ADMITS: VERSION 2.0
AUTOMATED TRAVEL ORDER SYSTEM ATOS: VERSION 040-05.04.05 OR 5.4.5
AIRCRAFT WEIGHT AND BALANCE AWBS: VERSION 8.1 (VERSION 9.1 WHEN CERTIFIED)
AVIATION MAINTENANCE MANAGEMENT AV3M: VERSION 004-14.00.00
CAREER INFORMATION CIPM 99: VERSION 1.0D-5
MAINTENANCE AUDITING SYSTEM CSEC: VERSION 1.1 (VERSION 2H, 2K WHEN CERTIFIED)
DEFENSE REQUISITIONING SYSTEM DAMES: VERSION 2.11.046
DEFENSE PROPERTY ACCOUNTING SYSTEM DPAS: VERSION 15.0.14 (MYEUREKA VERSION 6.1.313 AND SUPRA NT VERSION 36038.0)
PLAIN LANGUAGE ADDRESS SYSTEM DPVS: VERSION 6.0
PERSONNEL SECURITY EPSQ VERSION: 2.2 (SUBJECT EDITION AND SECURITY OFFICER EDITION)

HAZMAT MANAGEMENT HMIS: VERSION DEC2001 (INCLUDING FIRST EDITION HMIRS, VERSION TBD)
READINESS MANAGEMENT IRRS: VERSION 2.0.1
TRAVEL MANAGEMENT JFTR: VERSION 4.2 (FOLIO VIEWER)
LOGISTICS MANAGEMENT FEDLOG: VERSION 5.1
FITNESS REPORT PREPARATION NAVFIT98: VERSION 2.002.0021
DRUG SCREENING SYSTEM NDSP: VERSION 5.0
ELECTRONIC TRAINING SYSTEM NEETS: VERSION 1.0
MAINTENANCE READINESS MANAGEMENT RMSWIN: VERSION 8.0
AVIATION REPORTING SHARP: VERSION 4.0.3 SR1
MEDICAL MANAGEMENT SAMS: VERSION 25.08.02.00
NAVAL MESSAGE PREPARATION TURBOPREP VERSION 2.02A-5N (INCLUDING TURBOPREP PATCH A)
B. COGNIZANT DESIGN ACTIVITIES SHOULD ENSURE THAT THE MOST RECENT VERSION/UPDATE IS RELEASED TO SITES AS QUICKLY AS POSSIBLE. ALL REQUIREMENTS PROMULGATED IN REF B MUST BE MET PRIOR TO RELEASE.
C. IF AN ECHELON II COMMANDER REQUIRES AN ADDITIONAL VERSION OF AN APPLICATION LISTED IN PARA 4.A OR OTHER APPLICATIONS PERFORMING THE SAME FUNCTION, THE ECHELON II COMMANDER MUST REQUEST THIS EXCEPTION SEPARATELY FROM BOTH THE NAVY INFORMATION OFFICER AND APPLICABLE FUNCTIONAL AREA MANAGER. ANY EXCEPTION REQUEST SHOULD INCLUDE THE NUMBER OF LICENSES HELD FOR EACH VERSION, THE NUMBER OF ACTUAL USERS OF EACH VERSION, THE PLAN FOR MIGRATING TO THE CORRESPONDING APPLICATION LISTED IN PARAGRAPH 4.A AND JUSTIFICATION FOR INCLUDING THE APPLICATION FOR TRANSITION TO NMCI OR RETAINING THE APPLICATION FOR USE ON IT21 OR OCONUS BLII NETWORKS (INCLUDE THE UNIQUE FUNCTION BEING PERFORMED BY THIS OTHER APPLICATION AND WHY IT IS OPERATIONALLY REQUIRED).

5. THIS MESSAGE WILL BE UPDATED TO REFLECT THOSE CHANGES IDENTIFIED BY FUNCTIONAL AREA MANAGERS AS THEY DEVELOP THEIR RESPECTIVE APPLICATION AND DATABASE PORTFOLIOS.//

BT
#0309
NNNN

D5. Navy CNO 031345Z AUG 01

Subject: NMCI LEGACY APPLICATIONS//

031345Z AUG 01
UNCLAS

MSGID/GENADMIN/CNO N09T/005-01//

SUBJ/NMCI LEGACY APPLICATIONS//

REF/A/DOC/DON CIO/YMD:20010423//
REF/B/GENADMIN/CNO WASHINGTON DC/061414ZJUL2001/09T//
REF/C/GENADMIN/PEO IT WASHINGTON DC/282200ZFEB2001//
REF/D/DOC/SPAWARSYSCOM/13JUL2001//

NARR/REF A IS DON CIO POLICY MEMO CALLING FOR DEPARTMENT-WIDE REDUCTION OF LEGACY APPLICATIONS. REF B IS NAVY CIO MESSAGE 003-01 THAT PROVIDES GUIDANCE FOR NMCI TRANSITION OF LEGACY APPLICATIONS. REF C IS PEO IT MESSAGE THAT PROVIDES AN OVERVIEW OF THE PROCESS AND PROCEDURES TO SUPPORT THE ACCESS OF LEGACY APPLICATIONS UNDER NMCI. REF D IS THE NMCI LEGACY APPLICATIONS TRANSITION GUIDE VERSION 2.0.//

POC/ALAND, DAVID/CAPT/OPNAV NAVY CIO/-/TEL:703-604-6880// AMPN/EMAIL: ALAND.DAVID@HQ.NAVY.MIL//

POC/LAWAETZ,ALLIE/CIV/PEO IT/-/TEL:703-601-4750//
AMPN/EMAIL:LAWAETZA@SPAWAR.NAVY.MIL//

RMKS/1. THIS IS NAVY CIO MESSAGE 005/01 WHICH PROVIDES MANDATORY REQUIREMENTS FOR NMCI LEGACY APPLICATIONS TRANSITION, AMPLIFYING REFS A THRU D. LESSONS LEARNED SHOW THAT LEGACY APPLICATION CERTIFICATION IS THE CRITICAL PATH FOR NMCI TRANSITION. WE HAVE MORE COTS AND GOTS APPLICATIONS CURRENTLY IN USE THAN IS EITHER EFFICIENT OR AFFORDABLE. NMCI TRANSITION OFFERS AN OPPORTUNITY TO PROFOUNDLY IMPROVE THIS, BUT REQUIRES IMMEDIATE ACTION. ECHELON II COMMANDERS ARE EACH RESPONSIBLE FOR THE IDENTIFICATION, RATIONALIZATION, AND SUBMISSION FOR CERTIFICATION OF APPLICATIONS, VIA A PROCESS THAT INCLUDES INTEGRATION, CONSOLIDATION, AND ELIMINATION OF APPLICATIONS AND DATABASES. INDIVIDUAL SITE COMMANDERS ARE RESPONSIBLE FOR MEETING PRESCRIBED DEADLINES AND GOALS IN SUPPORT OF THEIR ECHELON II COMMANDERS.

2. ACTION:

A. ALL ECHELON II COMMANDERS MUST SUBMIT A REPORT, INCLUDING AN INITIAL APPLICATION INVENTORY, IAW REF A. A REPORT TEMPLATE WILL BE PROVIDED SEPARATELY. IOT SUPPORT NMCI SCHEDULES, THIS REPORT IS NOW REQUIRED NLT 01OCT01.

B. REFS B THRU D DETAIL THE TRANSITION PROCESS FOR LEGACY APPLICATIONS TO NMCI, AND IS AMPLIFIED BELOW. WAIVERS TO THESE REQUIREMENTS WILL BE AT THE DISCRETION OF THE NAVY CIO, OPNAV 09T.

(1) 120 DAYS PRIOR TO ASSUMPTION OF RESPONSIBILITY (AOR) BY THE INFORMATION STRIKE FORCE (ISF), COMMENCE THE TRANSITION PROCESS TO INCLUDE VALIDATION OF THE SITE APPLICATION INVENTORY. PRIOR TO THIS, INITIAL RATIONALIZATION AGAINST MISSION REQUIREMENTS AND COMMON BUSINESS RULES (PROVIDED SEPARATELY) AND

PRESURVEY QUESTIONNAIRES (PSQ'S) MUST BE COMPLETED. DELIVERY TO ISF OF THIS RATIONALIZED LIST OF APPLICATIONS SHOULD ALSO COMMENCE.

(2) 60 DAYS PRIOR TO AOR DELIVER THE COMPLETED LIST OF ALL COTS AND GOTS APPLICATIONS THAT WILL BE REQUIRED TO OPERATE ON NMCI. 50 PERCENT OF ALL GOTS APPS MUST BE DELIVERED TO THE ISF CERTIFICATION LABORATORY AND ACCEPTED.

(3) 45 DAYS PRIOR TO AOR, 75 PERCENT OF IDENTIFIED APPLICATIONS (COTS AND GOTS) SHOULD BE DELIVERED AND ACCEPTED FOR CERTIFICATION.

(4) 30 DAYS PRIOR TO AOR ALL REMAINING IDENTIFIED APPLICATIONS (COTS AND GOTS) MUST BE SUBMITTED AND ACCEPTED FOR CERTIFICATION. APPLICATIONS NOT SUBMITTED BY THIS DEADLINE WILL NOT TRANSITION TO NMCI AT THE SCHEDULED CUTOVER DATE.

(5) ALL FIRST INCREMENT SITES THAT HAVE NOT DELIVERED THEIR SURVEYS/INVENTORIES AND APPLICATIONS MUST COMPLETE AND DELIVER THEM WITHIN 30 DAYS FROM RECEIPT OF THIS MESSAGE.

(6) SOME SECOND INCREMENT SITES WITH AOR IN OCT/NOV 01 ARE ALREADY WITHIN THE 120 AND/OR 60 DAY DEADLINES. FOR THESE SITES, INVENTORY MUST BEGIN IMMEDIATELY, AND RATIONALIZED LISTS ARE DUE NO LATER THAN SCHEDULED AOR DATE. ALL APPLICATIONS MUST BE PROVIDED TO ISF AND ACCEPTED NO LATER THAN 30 DAYS AFTER AOR.

3. THE NMCI LEGACY APPLICATIONS TRANSITION PROCESS PROVIDES ECHELON II COMMANDS THE OPPORTUNITY TO ACHIEVE DISCIPLINE IN THEIR IT APPLICATIONS ENVIRONMENT. SOME COMMANDS ARE ALREADY SUCCEEDING AT THIS AND HAVE REALIZED SUBSTANTIAL LEGACY APPLICATION REDUCTIONS. PROACTIVE PARTICIPATION AND COLLABORATION WITH THE ISF IS ESSENTIAL. COMMANDERS ARE ACCOUNTABLE FOR THE SUCCESSFUL OPERATIONAL TRANSITION OF THEIR COMMANDS AND COMPLIANCE WITH THE PROCEDURES OUTLINED IN THIS MESSAGE AND REFS A THRU D. SPECIFIC COMMAND AOR SCHEDULES ARE AVAILABLE AT [QUOTE] WWW.EDS.COM/NMCI/TRANSITION.HTM [UNQUOTE] ALL LOWER CASE.
4. I WILL BE INDIVIDUALLY CONTACTING EVERY ECHELON II COMMANDER IN THE NEXT WEEK TO EMPHASIZE THE IMPORTANCE OF THIS MESSAGE. YOUR PERSONAL FEEDBACK IS ENCOURAGED AT ANY TIME. RELEASED BY VADM R.W. MAYO, NAVY CIO.//
BT
#0503
NNN

D6. 252250Z FEB 02 (25 Feb 02 2250Z)

From: CNO Washington
Subject: NMCI Legacy Application Transition Process

UNCLAS
MSGID/GENADMIN/CNO N09T/001-02//
SUBJ/NMCI LEGACY APPLICATIONS TRANSITION PROCESS//
REF/A/GENADMIN/CNO 09T WASHINGTON DC/061414ZJUL2001/003-01//
REF/B/GENADMIN/CNO 09T WASHINGTON DC/031345ZAUG01/005-01//
NARR/REFS A AND B ARE NAVY CIO MESSAGES 003-01 AND 005-01 AND PROVIDE GUIDANCE FOR NMCI TRANSITION OF LEGACY APPLICATIONS AND DIRECTED A ONE-TIME INVENTORY AND REPORTING OF LEGACY APPLICATIONS AT ALL ECHELON II COMMANDS.//
POC/ALAND, DAVID/CAPTAIN/OPNAV NAVY CIO/LOC: WASHINGTON DC/TEL: 703-604-6880//
AMPN/EMAIL: ALAND.DAVID@HQ.NAVY.MIL//
RMKS/1. EXECUTIVE SUMMARY. THE TRANSITION OF LEGACY APPLICATIONS TO NMCI IS A CRITICAL STEP FORWARD IN OUR ABILITY TO REALISTICALLY PERFORM INFORMATION RESOURCE MANAGEMENT. IT IS A LEADERSHIP ISSUE WHICH REQUIRES YOUR IMMEDIATE AND DIRECT ATTENTION. STATUS OF EACH ECHELON II COMMAND'S IDENTIFICATION, RATIONALIZATION, AND SUBMISSION OF APPLICATIONS FOR CERTIFICATION AND ACCREDITATION WILL BE REPORTED TO THE CNO AND SECNAV ON A WEEKLY BASIS. THIS MESSAGE BOTH MANDATES THE USE OF THE LEGACY APPLICATION TRANSITION GUIDE (LATG) AND MODIFIES LATG, PROVIDING DETAILED SUBMISSION DATES AND PROCEDURES THAT MUST BE FOLLOWED. THE MODIFICATION OF THE LATG SEPARATES THE NMCI CERTIFICATION PROCESS FROM THE FINAL ACCREDITATION PROCESS AND DELIVERS APPLICATIONS WHICH WILL OPERATE ON NMCI SEATS WITHOUT COMPROMISING SECURITY. REGRET THE LENGTH OF MESSAGE BUT THIS PROCESS CHANGE REQUIRES DETAIL AND CLARITY.
2. ECHELON II COMMANDERS ARE EACH RESPONSIBLE FOR THE IDENTIFICATION, RATIONALIZATION, AND SUBMISSION FOR CERTIFICATION AND ACCREDITATION OF THEIR APPLICATIONS. A CENTRAL DATABASE HAS BEEN ESTABLISHED FOR ALL NAVY APPLICATIONS. ACCESS TO THE DATABASE IS VIA A WEBSITE REQUIRING A USER PASSWORD. A SEPARATE MESSAGE WILL PROVIDE INFORMATION ON HOW ACCESS TO THE DATABASE CAN BE OBTAINED VIA EACH INDIVIDUAL'S ECHELON II COMMAND TO READ AND/OR WRITE TO THE DATABASE. A REVIEW OF THIS DATABASE INDICATES THAT MOST NMCI INCREMENT 1.0 AND 1.5 COMMANDS HAVE NOT COMPLETED THE REQUIRED DATA SUBMISSION IN SUPPORT OF NMCI IMPLEMENTATION. ADDITIONALLY, MOST COMMANDS SCHEDULED FOR NMCI INCREMENT 2.0 AND BEYOND HAVE SUBMITTED INCOMPLETE DATA WHICH COULD IMPACT NMCI IMPLEMENTATION. SITE TRANSITION EXECUTION MANAGER (STEM), ENTERPRISE APPLICATIONS GROUP FOR LEGACY & EMERGING (EAGLE) AND INFORMATION ASSURANCE TIGER TEAM (IATT) PERSONNEL HAVE BEEN FIELDED TO ASSIST TRANSITIONING SITES WITH THIS TASK. HOWEVER, THE SPEED AT WHICH LEGACY APPLICATIONS ARE IDENTIFIED, RATIONALIZED (REDUCED IN NUMBER), TESTED, CERTIFIED, AND ACCREDITED MUST BE IMPROVED. THERE ARE THREE KEYS TO IMPROVING THIS PROCESS. THE FIRST IS TO ENSURE EACH ECHELON II COMMAND MAINTAINS THEIR APPLICATION DATA CURRENT AND ACCURATE IN THE APPLICATION DATABASE TO ELIMINATE DUPLICATION OF EFFORT ACROSS THE NAVY ENTERPRISE. APPLICATIONS CERTIFIED AND ACCREDITED UNDER THE LATG PROCESS DO NOT REQUIRE DUPLICATE CERTIFICATION AND ACCREDITATION AT SUBSEQUENT COMMANDS/SITES. (REQUEST FOR SERVICE (RFS) SUBMISSION IS STILL REQUIRED BY SUBSEQUENT COMMANDS/SITES TO DOCUMENT APPLICATION

USE AND PREVIOUSLY ACCOMPLISHED CERTIFICATION.) THE SECOND KEY IS A REDUCTION IN THE NUMBER OF LEGACY APPLICATIONS ACHIEVED BY ECHELON II RATIONALIZATION AND NAVY TRIAGE PROCESS. (DATA COLLECTED THUS FAR SHOWS APPROXIMATELY 10-20 PERCENT OF ALL APPLICATIONS CURRENTLY CERTIFIED AND ACCREDITED DO NOT HAVE ANY IDENTIFIED USERS, WHICH HAS RESULTED IN A NEEDLESS EXPENDITURE OF SCARCE RESOURCES.) THE THIRD KEY IS A REDUCTION IN THE REQUIREMENTS FOR INCLUDING LEGACY APPLICATIONS AT NMCI SEAT CUTOVER, BUT NOT A REDUCTION IN REQUIREMENTS FOR LEGACY APPLICATION ACCREDITATION. IN ORDER TO REDUCE THE IMPACT TO NMCI SEAT ROLLOUT, THE APPLICATION TRANSITION PROCESS IS MODIFIED PER PARAGRAPH 3 AND ACTION IDENTIFIED IN PARAGRAPH 4 IS MANDATORY.
3. LEGACY APPLICATION TRANSITION PROCESS MODIFICATION. THE FOLLOWING PROCESS MODIFICATIONS ARE EFFECTIVE IMMEDIATELY AND SHALL BE FOLLOWED IN CONJUNCTION WITH THE LATG:
A. GENERAL: THE CURRENT LEGACY APPLICATION PROCESS ENTAILS SITE IMPLEMENTATION VICE COMMAND IMPLEMENTATION DURING THE LEGACY APPLICATION IDENTIFICATION AND THE RATIONALIZATION PROCESSES AND THE COMPLETION OF THE CERTIFICATION PROCESS (COMPATIBILITY WITH THE NMCI OPERATING ENVIRONMENT) AND THE SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA) PRIOR TO COMMENCING CUTOVER OF SEATS. THE NEW PROCESS REQUIRES ECHELON II CHAIN OF COMMAND (COC) INVOLVEMENT DURING THE IDENTIFICATION AND THE RATIONALIZATION PROCESSES AND DIVIDES THE CERTIFICATION PROCESS INTO TWO PHASES, THE NMCI CERTIFICATION PHASE AND THE RISK MITIGATION (ACCREDITATION) PHASE.
B. IDENTIFICATION AND RATIONALIZATION: NEW PROCESS REQUIRES SUBORDINATE COMMANDS TO SUBMIT THEIR RATIONALIZED LIST OF APPLICATIONS VIA THEIR COC TO THEIR ECHELON II FOR RATIONALIZATION ACROSS THE ECHELON II'S ENTERPRISE. IT REQUIRES A WEEKLY REPORTING OF EACH COMMAND'S PROGRESS IN COMPLETING SUBMISSION REQUIREMENTS FOR THE CERTIFICATION PROCESS.
C. NMCI CERTIFICATION: IN THE NEW PROCESS THE NMCI CERTIFICATION PHASE INCLUDES THE DEVELOPMENT OF RATIONALIZED LISTS OF APPLICATIONS, THE SUBMISSION OF REQUESTS FOR SERVICE (RFS) AND MEDIA FOR THOSE APPLICATIONS, THE SUBMISSION OF THE CERTIFICATION PHASE ENGINEERING REVIEW QUESTIONNAIRE (ERQ), THE ACTUAL CERTIFICATION TESTING OF THE APPLICATION, AND THE SUBMISSION OF AN IATT VULNERABILITY ASSESSMENT LETTER TO THE NMCI DESIGNATED APPROVAL AUTHORITY (DAA) (CAPTAIN BOB WHITKOP, COMMANDER NAVY NETWORK OPERATIONS COMMAND (CNNOC)). THE NMCI CERTIFICATION PROCESS CULMINATES IN THE ISSUANCE OF AN INTERIM AUTHORITY TO OPERATE (IATO) LETTER FROM THE NMCI DAA. THE IATO WILL CONTAIN LIMITATIONS ON THE OPERATION OF EACH APPLICATION AND REQUIRE INFORMATION ASSURANCE RISK MITIGATION ACTIONS TO BE ACCOMPLISHED WITHIN TIME SPECIFIED IN PARAGRAPH 3.D. D. CERTIFICATION PROCESS CHANGES: THE PACING FACTOR FOR MUCH OF THE NMCI CERTIFICATION PROCESS WILL CONTINUE TO RELY ON OBTAINING THE RFS, MEDIA, AND COMPLETION OF THE ERQ FOR EACH COMMAND'S APPLICATIONS AT EACH SITE. IT IS ESSENTIAL THAT BOTH THE APPLICABLE ECHELON II COMMANDS AND THE SITE ENSURE THIS DATA IS SUBMITTED IN A TIMELY MANNER IN ORDER TO SUPPORT THE NMCI IMPLEMENTATION SCHEDULE. THE NMCI CERTIFICATION ERQ AND THE RISK MITIGATION (ACCREDITATION) ERQ INCLUDE ALL THE DATA REQUIREMENTS OF THE ORIGINAL ERQ. HOWEVER, THE NMCI CERTIFICATION ERQ HAS BEEN SIGNIFICANTLY REDUCED IN SIZE AND COMPLEXITY TO EXPEDITE THE SEAT CUTOVER PROCESS, WHILE COLLECTING THE NECESSARY INFORMATION TO ENSURE NETWORK SECURITY IS MAINTAINED AT CUTOVER. THE NMCI CERTIFICATION TESTING HAS ALSO BEEN STREAMLINED. EACH APPLICATION

WILL UNDERGO AN ON SITE POP-IN-A-BOX (PIAB) TEST TO ENSURE COMPATIBILITY WITH THE MICROSOFT WIN2K OPERATING SYSTEM, DESKTOP GROUP POLICY OBJECT (GPO), SECURITY COMPONENTS AND SETTINGS. THE PIAB TESTING WILL ALSO PROVIDE CONNECTIVITY REQUIREMENTS BETWEEN CLIENT AND SERVER AT THE PROTOCOL, SERVICE AND PORT LEVEL. ADDITIONAL PERSONNEL AND EQUIPMENT WILL BE ASSIGNED BY THE PMO AND THE NMCI CONTRACTOR TO THE EXISTING TEAMS IN ORDER TO CONDUCT THIS ON SITE PIAB TESTING AND DOCUMENTATION AT A GREATER NUMBER OF SITES CONCURRENTLY. BASED ON THIS INFORMATION GAINED FROM THE PIAB TESTING, THE IATT WILL PROVIDE A RISK ASSESSMENT OF EACH APPLICATION AS FOLLOWS:
-- LOW RISK - COMPLIANT WITH NAVY/MARINE CORPS ENCLAVE PROTECTION POLICY AND ACCREDITED.
-- MEDIUM RISK - OUTBOUND TCP COMMUNICATION REQUIREMENTS NOT ALREADY PERMITTED.
-- HIGH RISK - TWO WAY IP/TCP/UDP COMMUNICATION REQUIREMENTS NOT ALREADY PERMITTED.
-- VERY HIGH RISK - UNACCEPTABLE PROTOCOLS OR REQUIREMENTS. MANDATORY KIOSK MITIGATION UNTIL DISCONTINUED OR REENGINEERED. THESE RISKS WILL BE CAPTURED BY THE ON-SITE IATT REPRESENTATIVES AND FORWARDED TO THE NMCI DAA IN THE VULNERABILITY ASSESSMENT LETTER. WHEN ALL CERTIFICATION TESTING RESULTS FOR A SITE ARE AVAILABLE TO THE NMCI DAA, HE WILL ISSUE A TYPE ACCREDITED BOUNDARY 2 FIREWALL POLICY FOR THE SITE AND ISSUE AN IATO COVERING THE SUITE OF APPLICATIONS AT THAT SITE. IN ADDITION TO THE VULNERABILITY ASSESSMENT RESULTS DISCUSSED ABOVE, THE IATO WILL CONSIDER THE STATE OF AVAILABLE SSAA DOCUMENTATION FOR EACH APPLICATION IN ACCORDANCE WITH THE FOLLOWING BOUNDARY 1 FIREWALL COMPLIANCE CATEGORIES:
- CATEGORY 1 - CLIENT APPLICATION IS NMCI CERTIFIED AND USES TRUSTED COMMUNICATIONS WITH THE SUPPORTING SERVER. EITHER THE SERVER APPLICATION OR BOTH CLIENT AND SERVER PORTIONS OF THE APPLICATION HAVE CERTIFICATION AND ACCREDITATION (C&A) PACKAGES AND CAN BE MOVED INTO NMCI TRUSTED ENCLAVE. SSAA PACKAGE IS COMPLETE AND THE APPLICATION IS ACCREDITED.
- CATEGORY 2 - CLIENT APPLICATION IS NMCI CERTIFIED, BUT CONCERNS EXIST ABOUT COMMUNICATIONS WITH THE SERVER BECAUSE OF A LACK OF COMPLETED DOCUMENTATION (NO DEPARTMENT OF DEFENSE (DOD) C&A.) SERVER APPLICATION IS NMCI CERTIFIED, BUT CONCERNS EXIST WITH THE SERVER'S COMMUNICATION WITH OTHER SERVERS AND/OR CLIENTS BECAUSE OF THE LACK OF COMPLETED DOCUMENTATION (NO DOD C&A.) NO BOUNDARY 2 MODIFICATIONS ARE REQUIRED. RISK IS MINIMIZED IF BOTH CLIENT AND SERVER ARE PLACED WITHIN NMCI ENCLAVE VICE LEAVING THE SERVER OUTSIDE THE NMCI ENCLAVE.
- CATEGORY 3 - CLIENT IS NMCI CERTIFIED, BUT SERVER HAS UNTRUSTED COMMUNICATION REQUIREMENTS TO NON-NMCI USERS FOR THE RISK MITIGATION (ACCREDITATION) PHASE OR LONGER. SERVER APPLICATION IS NMCI CERTIFIED, BUT THE SERVER HAS UNTRUSTED COMMUNICATION REQUIREMENTS TO NON-NMCI SERVERS AND/OR USERS FOR THE RISK MITIGATION (ACCREDITATION PHASE OR LONGER. BOUNDARY 2 FIREWALL MODIFICATION IS REQUIRED.
- CATEGORY 4 - CLIENT APPLICATION MAY OR MAY NOT BE CERTIFIED, AND THERE IS UNTRUSTED COMMUNICATIONS BETWEEN CLIENT AND SERVER OR SERVER AND SERVER OR APPLICATION CLIENT/SERVER IS ACCESSIBLE TO THE GENERAL PUBLIC. NO DOD C&A. SYSTEM CAN EITHER BE SUNSET-ED OR KIOSKED. A RULE SET GOVERNING SUPPORT FOR KIOSKED APPLICATIONS WILL BE PROVIDED SEPARATELY. BASED ON BOUNDARY 1 FIREWALL COMPLIANCE CATEGORY AND THE RISK LEVEL, THE NMCI DAA WILL ISSUE AN IATO

REQUIRING SPECIFIC ACTIONS AND LIMIT THE AUTHORITY TO OPERATE FOR A SPECIFIED TIME PERIOD AS FOLLOWS:
CATEGORY 1 - LENGTH OF AUTHORITY TO OPERATE (ATO) (NORMALLY 3 YEARS).
CATEGORY 2 - ONE YEAR
CATEGORY 3 - SUBMIT PLAN OF ACTION MILESTONES (POA&M) FOR MIGRATION VIA APPLICABLE ECHELON II COMMAND WITHIN SIX MONTHS TO NAVY CIO FOR APPROVAL/DISAPPROVAL AND ANNUAL REVIEW.
CATEGORY 4 - POA&M SUBMITTED FOR MITIGATION/MIGRATION VIA APPLICABLE ECHELON II DUE WITHIN THREE MONTHS TO NAVY CIO. MIGRATION/TERMINATION MUST BE COMPLETED WITHIN NINE MONTHS.
E. RISK MITIGATION (ACCREDITATION): THE SECOND PHASE OF THE PROCESS COMMENCES AFTER NMCI SEAT CUTOVER AND INVOLVES THE COMPLETION OF THE RISK MITIGATION (ACCREDITATION) ERQ, FURTHER DEVELOPMENT OF RISK MITIGATION STRATEGIES, SUBMISSION OF POA&M FOR EACH APPLICABLE APPLICATION IAW IATO REQUIREMENTS, EXECUTION OF APPLICATION MITIGATION ACTION AND COMPLETION OF SSAA DOCUMENTATION. FAILURE TO COMPLETE REQUIRED MITIGATION ACTIONS (SUBMIT POA&M AND MEET TIMELINES) WILL RESULT IN EITHER DENIAL OF APPLICATION USE ON NMCI BY THE NAVY CIO OR POTENTIAL ADDITIONAL MITIGATION REQUIREMENTS. THE PRIMARY TASKS IN THIS PHASE ARE THE MITIGATIONS OF THE RISKS IDENTIFIED DURING THE CERTIFICATION PHASE AND THE COMPLETION OF THE SSAA DOCUMENTATION REQUIRED FOR CERTIFICATION. THERE HAVE BEEN MANY TECHNIQUES ALREADY DEVELOPED BY THE NMCI CONTRACTOR (INFORMATION STRIKE FORCE (ISF)) FOR CATEGORY 3 APPLICATIONS TO MITIGATE RISKS UNTIL THE SERVER CAN BE TRANSITIONED INTO THE NMCI ENCLAVE. COMPLETION OF RISK MITIGATION IS THE RESPONSIBILITY OF THE APPLICABLE ECHELON II COMMAND, INCLUDING APPLICABLE SUBORDINATE COMMANDS, THE CENTRAL DESIGN ACTIVITY (AS DESIGNATED IN PARAGRAPH 4.B) AND THE ISF. SSAA DOCUMENTATION IS SUBMITTED BY ECHELON II COMMAND OR CDA, AS APPROPRIATE, TO NMCI PROGRAM MANAGEMENT OFFICE (PMO) FOR INITIAL REVIEW AND EVALUATION PRIOR TO SUBMISSION TO THE NMCI DAA FOR APPROVAL. FOR CATEGORY 4 APPLICATIONS, A RECOMMENDATION TO MIGRATE OR TERMINATE THE APPLICATION WILL BE MADE AND APPROVED BY THE NAVY CIO. FOR ALL APPLICATIONS THAT ARE TO REMAIN IN THE NMCI, THE SSAA DOCUMENTATION WILL BE DEVELOPED BY THE ECHELON II COMMAND OR CDA, AS APPROPRIATE, AND SUBMITTED TO NMCI PMO FOR INITIAL REVIEW AND EVALUATION PRIOR TO SUBMISSION TO THE NMCI DAA FOR APPROVAL.
F. NAVY TRIAGE PROCESS: AN APPLICATION TRIAGE PROCESS, WHICH WILL BE DESIGNED TO REDUCE THE OVERALL NUMBER OF NAVY APPLICATIONS, WILL RUN CONCURRENTLY WITH NMCI CERTIFICATION AND THE RISK MITIGATION (ACCREDITATION) PHASES AT THE ECHELON II AND NAVY CIO LEVEL. THE PRODUCT OF THE NMCI CERTIFICATION PHASE, BOUNDARY 1 FIREWALL COMPLIANCE CATEGORY AND RISK LEVEL, WILL BE USED TO ESTABLISH PRIORITIES AND IDENTIFY APPLICATIONS FOR ELIMINATION DURING THE TRIAGE PROCESS. THIS PROCESS WILL BE ADDRESSED SEPARATELY.
4. ACTION AND RESPONSIBILITIES. IN ORDER FOR THE MODIFIED PROCESS DEFINED IN PARAGRAPH 3 TO BE EFFECTIVE THE FOLLOWING SPECIFIC ACTION AND RESPONSIBILITIES ARE REQUIRED:
A. ECHELON II ARE RESPONSIBLE TO ENSURE THEY AND THEIR SUBORDINATE COMMANDS COMPLY WITH THE FOLLOWING:
(1) 60 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND DELIVERS THE COMPLETED LIST OF ALL COTS AND GOTS APPLICATIONS REQUIRED TO OPERATE ON NMCI AND RATIONALIZED BY THEIR ECHELON II COMMAND. **50 PERCENT** OF ALL GOTS APPLICATIONS MUST BE DELIVERED AND ACCEPTED BY THE ISF FOR CERTIFICATION.

(2) 45 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND SHALL HAVE **75 PERCENT** OF IDENTIFIED APPLICATIONS (COTS AND GOTS) DELIVERED AND ACCEPTED FOR CERTIFICATION.
(3) 30 DAYS PRIOR TO AOR, THE APPLICABLE COMMAND SHALL ENSURE **ALL** REMAINING IDENTIFIED APPLICATIONS (COTS AND GOTS) MUST BE SUBMITTED AND ACCEPTED FOR CERTIFICATION. APPLICATIONS NOT SUBMITTED BY THIS DEADLINE WILL NOT TRANSITION TO NMCI ON THE SCHEDULED CUTOVER DATE.
(4) 14 DAYS PRIOR TO START OF CUTOVER, ALL APPLICATIONS REQUIRED FOR CUTOVER ARE CERTIFIED.
(5) ALL INCREMENT 1.0 COMMANDS MUST HAVE COMPLETED SUBMISSION OF THEIR FINALIZED RATIONALIZED APPLICATION LIST TO NMCI PMO. THE APPROPRIATE ECHELON II COMMAND SHOULD HAVE PREVIOUSLY APPROVED THIS RATIONALIZED LIST OR DO SO NLT 21 MARCH 2002.
(6) ALL INCREMENT 1.5 COMMANDS MUST HAVE THEIR RATIONALIZED LIST OF APPLICATIONS SUBMITTED VIA THEIR APPLICABLE ECHELON II COMMAND NLT 21 MARCH 2002.
(7) APPLICATIONS SHALL BE SUBMITTED AS NOTED ABOVE USING THE REQUEST FOR SERVICE (RFS) AND CERTIFICATION PHASE ERQ. ALL DATA ELEMENTS IDENTIFIED IN THE RFS AND IN THE CERTIFICATION PHASE AND THE RISK MITIGATION (ACCREDITATION) PHASE ERQ ARE MANDATORY IN ORDER FOR THIS SUBMISSION TO BE CONSIDERED COMPLETE.
B. DESIGNATION OF CDA: CRITICAL TO THE LEGACY APPLICATION PROCESS IS THE ASSIGNMENT OF RESPONSIBILITY FOR EVERY APPLICATION TO BE CERTIFIED OR ACCREDITED. THIS MESSAGE ASSIGNS RESPONSIBILITIES TO CENTRAL DESIGN ACTIVITIES (CDA) AND DETAILS THE PROCESS TO ASSIGN CDA RESPONSIBILITIES WHEN A DESIGNATED CDA DOES NOT EXIST. IN ORDER TO EXPEDITE THE CERTIFICATION AND ACCREDITATION PROCESS, CDA(S) FOR APPLICATIONS WHICH EXIST AT MORE THAN ONE SITE, SHALL SUBMIT SSAA DOCUMENTATION FOR THE APPLICABLE APPLICATION ONCE VICE REQUIRING DUPLICATION OF CDA RESPONSIBILITIES AT MULTIPLE SITES BY MULTIPLE ECHELON II COMMANDS. CDA HAS PRINCIPAL RESPONSIBILITY FOR DESIGN, DEVELOPMENT, DOCUMENTATION, AND LIFE CYCLE MAINTENANCE OF APPLICATIONS, INCLUDING INITIAL PRODUCT DELIVERY AND DISTRIBUTION OF UPDATES. ADDITIONALLY, CDA(S) RESOURCE AND MAINTAIN HELP DESK SERVICES FOR THEIR APPLICATIONS. THE PRIMARY DON CDA(S) ARE CONTROLLED BY NAVSEA, NAVAIR, SPAWAR, NAVSUP, NAVFAC, CNET, MARINE CORPS SYSTEMS COMMAND AND DISTRIBUTED TO SOME OF THEIR SUBORDINATE COMMANDS (E.G. NAVSUP HAS FLEET MATERIALS SUPPORT OFFICE (FMSO) PROVIDE THEIR CDA RESPONSIBILITIES). THE FOLLOWING CATEGORIES OF APPLICATIONS AND THEIR ASSOCIATED CDA IDENTIFICATION AND DESIGNATION RESPONSIBILITY ARE ASSIGNED:
(1) NAVY SYSTEM COMMAND DEVELOPED GOTS - APPLICABLE SYSCOM IS RESPONSIBLE FOR IDENTIFICATION, DESIGNATION OF THE CDA AND ENSURING SUBSEQUENT CDA RESPONSIBILITIES ARE ACCOMPLISHED IAW THIS MESSAGE.
(2) MARINE CORPS SYSTEM COMMAND DEVELOPED GOTS - APPLICABLE NAVY ECHELON II IS RESPONSIBLE FOR REPORTING THE APPLICATION ASSOCIATED SYSCOM TO NAVY CIO, MARINE CORPS CIO OFFICE AND NMCI PMO. THE NAVY CIO WILL WORK WITH MARINE CORPS CIO OFFICE AND NMCI PMO FOR CDA IDENTIFICATION, DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(3) INDIVIDUAL COMMAND DEVELOPED GOTS - APPLICABLE ECHELON II IS RESPONSIBLE FOR IDENTIFICATION, DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(4) OTHER SERVICE/JOINT/OSD AND OTHER AGENCY DEVELOPED GOTS - APPLICABLE ECHELON II IS RESPONSIBLE FOR IDENTIFICATION OF THE APPLICATION AND ITS SOURCE TO NAVY CIO AND NMCI PMO. THE NAVY CIO WILL WORK WITH DON CIO AND NMCI PMO FOR IDENTIFICATION AND

DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(5) NON-GOVERNMENT, NON-COMMERCIAL PRODUCTS - APPLICABLE ECHELON II WHOSE SUBORDINATE COMMAND PURCHASED THE PRODUCT FOR USE IS RESPONSIBLE FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION.
(6) COMMERCIAL PRODUCTS (COTS) - APPLICABLE ECHELON II WHOSE SUBORDINATE COMMAND PURCHASED THE PRODUCT FOR USE IS RESPONSIBLE FOR IDENTIFICATION AND DESIGNATION OF THE CDA AND THE CDA'S COMPLETION OF REQUIRED ACTION. FOR APPLICATIONS CONTAINED IN THE NMCI BASIC DESKTOP SEAT, IDENTIFICATION AND DESIGNATION OF CDA IS NOT REQUIRED. IN THE FUTURE, AS ENTERPRISE APPLICATIONS ARE DESIGNATED AND CENTRALLY PURCHASED CDA RESPONSIBILITIES WILL BE ASSIGNED TO THE VENDOR AND INCLUDED IN THE ACQUISITION AGREEMENT.
C. ECHELON II AND CDA RESPONSIBILITIES: AS APPLICABLE, EACH ECHELON II COMMAND IS RESPONSIBLE FOR ENSURING THEIR CDA(S) SUBMIT THE APPLICATION SSAA DOCUMENTATION TO NMCI PMO. FOR EXAMPLE, THE CDA FOR THE NAVAL AIR LOGISTICS COMMAND MANAGEMENT INFORMATION SYSTEM (NALCOMIS) IS SPAWAR SO SPAWAR SHOULD ENSURE THE CDA FOR NALCOMIS COMPLIES WITH THE REQUIREMENTS OF THIS MESSAGE. AS A JOINT EXAMPLE, THE CDA FOR THE DEFENSE MESSAGE SYSTEM (DMS) IS DISA, SO ECHELON II REPORTS THE SOURCE OF DMS AS DISA AND THE NAVY CIO WILL WORK WITH DON CIO TO ENSURE DISA HAS THEIR DMS CDA COMPLY WITH THE REQUIREMENTS OF THIS MESSAGE. THESE KNOWN CDA(S) SHOULD BE PROVIDING THE REQUIRED SSAA DOCUMENTATION AND THE NMCI PMO WILL CONDUCT AN INITIAL REVIEW OF THE SSAA FOR CONSIDERATION AS ADEQUATE DOCUMENTATION FOR ALL NMCI COMMAND AND SITE IMPLEMENTATIONS. THIS CDA SUBMITTED SSAA DOCUMENTATION WILL BE EVALUATED AND ASSIGNED THE FOLLOWING STATUS: (A) SATISFACTORY AS A SSAA FOR NMCI, OR (B) NOT SATISFACTORY AS A SSAA FOR NMCI BUT DOES INCLUDE THE NECESSARY INFORMATION FOR COMPLETION OF THE NMCI CERTIFICATION PROCESS, OR (C) INCOMPLETE. SATISFACTORY SSAA'S WILL BE SUBMITTED TO THE NMCI CERTIFICATION AND ACCREDITATION REVIEW PANEL (NCARP) FOR ENTERPRISE ACCREDITATION. IF THIS CDA SUBMITTED SSAA DOCUMENTATION IS NOT A SATISFACTORY SSAA FOR NMCI OR IS INCOMPLETE, NMCI PMO WILL REPORT THIS TO THE NMCI DAA, THE LOCAL DAA(S) AND CAUSE A FORMAL MESSAGE TO BE PREPARED TASKING THE APPLICABLE CDA TO TAKE ACTION TO ENSURE MINIMUM REQUIREMENTS FOR SEAT CUTOVER ARE COMPLETED IMMEDIATELY. THE CDA MUST ENSURE SUBSEQUENT SSAA DOCUMENTATION IS COMPLETED IN ACCORDANCE WITH THE IATO TIME REQUIREMENTS FOR THE SPECIFIC APPLICATION. THE FOLLOWING SPECIFIC ACTION AND RESPONSIBILITIES NEED TO BE FOLLOWED BY THE CDA(S):
- MUST HAVE COMPLETED SUBMISSION OF AN RFS FOR EACH APPLICATION NLT 21 MARCH 2002 USING THE NMCI APPLICATION DATABASE. (THE 21 MARCH 2002 DATE DOES NOT APPLY TO AN APPLICATION, WHICH NEVER HAD A DESIGNATED CDA. FOR THESE APPLICATIONS, THE NEWLY DESIGNATED CDA SHOULD PROVIDE THE RFS DOCUMENTATION NLT 11 MAY 2002.)
- MUST HAVE COMPLETED SUBMISSION OF ALL CLIENT MEDIA TO THE ISF NLT 21 APRIL 2002. (THE 21 APRIL 2002 DATE DOES NOT APPLY TO AN APPLICATION WHICH NEVER HAD A DESIGNATED CDA. FOR THESE APPLICATIONS, THE NEWLY DESIGNATED CDA SHOULD PROVIDE THE CLIENT MEDIA NLT 11 MAY 2002.)
- FOR SUBSEQUENT UPGRADES/PATCHES TO EXISTING APPLICATIONS, MUST SUBMIT AN RFS USING THE NMCI APPLICATION DATABASE AND SUBMIT MEDIA TO THE ISF FOR CERTIFICATION. EACH CDA IS RESPONSIBLE FOR INDEPENDENT CERTIFICATION AND ACCREDITATION OF ANY CHANGES TO THEIR APPLICATIONS AS DESIGNATED BY THE NMCI

DAA. FURTHER DETAILS ON A NMCI FOLLOW-ON CERTIFICATION AND ACCREDITATION PROCESS ARE BEING DEVELOPED AND WILL BE PROVIDED SEPARATELY.
- MUST CHANGE APPLICATION DISTRIBUTION AND NOTIFICATION PROCESSES. FOR AN INTERIM PERIOD, THEY MUST DEVELOP PARALLEL PROCESSES FOR NMCI AND NON-NMCI SITES. FOR NMCI SITES, APPLICATIONS MUST NOT BE DELIVERED TO SITES WITHOUT FIRST UNDERGOING NMCI CERTIFICATION AND ACCREDITATION.
- MUST STANDARDIZE APPLICATIONS TO REDUCE MULTIPLE VERSIONS. IMPLEMENTATION OF APPLICATIONS ON NMCI SHOULD GREATLY FACILITATE THESE EFFORTS.
- MUST ENSURE DESIGNATED HELP DESK SUPPORT ACTIVITIES ARE WORKING SEAMLESSLY WITH NMCI HELP DESKS. WORKING GROUPS ARE IN THE PROCESS OF DEFINING NMCI AND LEGACY SYSTEM HELP DESK PROCESSES. EACH CDA WILL BE CONTACTED TO PARTICIPATE.
- MUST COMPLETE REQUIRED SSAA DOCUMENTATION FOR ALL APPLICATIONS INTENDED FOR CONTINUED USE ON NMCI. FOR INCREMENT 1.0 AND 1.5 SITES, THE SSAA DOCUMENT IS REQUIRED BY 01 AUGUST 2002. FOR ALL OTHER APPLICATIONS, THE SSAA IS REQUIRED NLT 01 SEPTEMBER 2002.
D. REPORTING: THE PRIMARY TOOL TO ENSURE ACCURATE REPORTING OF LEGACY APPLICATIONS STATUS IS THE NMCI DATABASE. EACH ECHELON II COMMAND WILL TAKE APPROPRIATE ACTION TO ENSURE ALL DATA ELEMENT ENTRIES ARE COMPLETE, ACCURATE, AND MAINTAINED CURRENT FOR THEIR COMMAND AND SUBORDINATE COMMANDS. THIS INCLUDES THE IDENTIFICATION OF EACH APPLICATION'S CDA. THE NMCI PMO WILL CONSOLIDATE THIS DATA FOR WEEKLY REPORTING TO SECNAV AND CNO. REPORTS WILL REFLECT STATUS OF RATIONALIZATION, RFS SUBMISSION, CERTIFICATIONS, ACTION PLANS, AND SSAA DOCUMENTATION.
5. SPECIFIC NAVY POLICY, GUIDANCE AND GOALS WILL BE PROVIDED SHORTLY CONCERNING THE FURTHER REDUCTION OF LEGACY APPLICATIONS AND THE ELIMINATION OF LEGACY NETWORKS REQUIRED TO SUPPORT KIOSKED APPLICATIONS.
6. THIS PROCESS MODIFICATION IS REQUIRED TO FACILITATE THE IMPLEMENTATION AND COMPLETION OF NMCI WITHIN DON. YOUR PERSONAL ATTENTION AND SUPPORT IS REQUESTED TO ENSURE SUCCESS.
7. RELEASED BY VADM R. W. MAYO, USN.//
BT
NNNN

D7. 241645Z FEB 03

Subject: DEFENSE MESSAGE SYSTEM (DMS) RELEASE 3.0 USER TRAINING

ROUTINE

R 241645Z FEB 03 PSN 938493S36

SUBJ: DEFENSE MESSAGE SYSTEM (DMS) RELEASE 3.0 USER TRAINING

Subject: NAVY NMCI LESSONS LEARNED REPOSITORY//
Importance: Low

BT
UNCLAS //N5000//

MSGID/GENADMIN/COMSPAWARSYSCOM/PMW164//
SUBJ/NAVY NMCI LESSONS LEARNED REPOSITORY//
REF/A/GENADMIN/COMSPAWARSYSCOM/241823ZDEC2002//
AMPN/REF (A) NAVY NMCI LESSONS LEARNED//
POC/MR. KEVIN MCNALLY/CIV NMCI PMO/COMSPAWARSYSCOM/-
/TEL:(619) 524-7580/EMAIL:KEVIN.MCNALLY@NAVY.MIL//

RMKS/1. IN AN EFFORT TO IMPROVE COMMUNICATIONS ACROSS THE ENTERPRISE, NAVY PMO IS LAUNCHING A NAVY NMCI LESSONS LEARNED REPOSITORY AS A PART OF THE DIRECTOR OF NMCI WEBSITE. THE INITIAL CAPABILITIES FOR THIS REPOSITORY ARE NOW AVAILABLE ON THE NMCI WEBSITE AT HTTP:/WWW.NMCI.NAVY.MIL UNDER THE TRANSITION TO NMCI, NAVY, AND LESSONS LEARNED MENU ITEMS. THIS SITE IS USERNAME AND PASSWORD PROTECTED. USERNAME: NMCI (LOWER CASE) **PASSWORD: TRANSITION** (LOWER CASE).

2. LESSONS LEARNED ARE DIVIDED INTO THREE CATEGORIES; PRE-CUTOVER, CUTOVER, AND POST CUTOVER. ADDITIONAL CATEGORIES WILL BE ADDED AS ADDITIONAL ENTERPRISE LESSONS ARE ACCUMULATED. LINKS ARE PROVIDED FOR USERS TO SUBMIT NEW LESSONS LEARNED, OR TO COMMENT ON A POSTED LESSON LEARNED. ALL COMMENTS AND NEW LESSONS LEARNED WILL BE REVIEWED FOR CONTENT AND, IF APPROPRIATE, POSTED IN THIS REPOSITORY.

3. A LESSON IS NOT TRULY LEARNED UNLESS IT HAS BEEN SHARED ACROSS THE ENTERPRISE FOR THE BENEFIT OF THOSE ABOUT TO EMBARK ON THE SAME JOURNEY. INITIAL INPUTS ON THE WEBSITE HAVE BEEN DEVELOPED FROM THE USER INPUTS AND EXPERIENCE GAINED HERE AT THE PROGRAM OFFICE. CNAL HAS BEEN PARTICULARLY HELPFUL WITH THEIR WELL-STRUCTURED
SUBMISSIONS. ALL CLAIMANTS ARE ENCOURAGED TO ACCESS THE SITE, SHARE ADDITIONAL LESSONS LEARNED, AND PROVIDE COMMENT TO ENHANCE EXISTING

LESSONS LEARNED. CLAIMANTS ARE ALSO REQUESTED TO PROVIDE COMMENTS OR SUGGESTIONS FOR THE IMPROVEMENT OF THIS LESSONS LEARNED REPOSITORY.

4. CAPT CRAIG MADSEN USN, NMCI NAVY PROGRAM MANAGER SENDS.//

BT

#6921
NNNN

D8. 202304Z MAY 02

SUBJ/NMCI 20K ROLLOUT EXECUTION ORDER//

Precedence: Priority
Date/Time Group202304Z MAY 02

Subject: NMCI 20K ROLLOUT EXECUTION ORDER//
UNCLAS
THIS IS A 3 SECTION MESSAGE COLLATED BY DMDS
MSGID/GENADMIN/PEO-IT WASHINGTON DC/0008//
SUBJ/NMCI 20K ROLLOUT EXECUTION ORDER//
RMKS/1. THIS NMCI EXECUTION ORDER OUTLINES COMMAND AND CONTROL (C2), ORGANIZATIONAL AND REPORTING REQUIREMENTS NECESSARY TO SUPPORT THE AGGRESSIVE ROLLOUT AND CUSTOMER USABILITY OF NMCI SEATS. IT ALSO IDENTIFIES THOSE SITES WHICH ARE CHARGED WITH ACTIVE CUTOVER IN THIRD QUARTER FY02.
2. BACKGROUND. AT THE 3 MAY 2002 SENIOR LEVEL REVIEW FOR NMCI, ASD C3I/DOD CIO AND USD AT&L GRANTED AUTHORITY FOR DON TO ORDER AN ADDITIONAL 100,000 NMCI SEATS. THIS MOVES NMCI OUT OF THE STRATEGIC PAUSE AND INTO THE FULL IMPLEMENTATION (ROLLOUT) PHASE. OUR NEXT STRATEGIC OBJECTIVE IS TO COMPLETE THE CUTOVER OF 20,000 NMCI SEATS NLT MID SUMMER AND DELIVER USABILITY ON THOSE SEATS IN ORDER TO SUPPORT REQUIRED SLA PERFORMANCE AND OPERATIONAL TESTING.
3. NMCI C2. NMCI ROLLOUT REQUIRES EFFICIENT AND EFFECTIVE C2. BASED ON LESSONS LEARNED FROM THE CONTRACTOR TEST AND EVALUATION PHASE, NMCI C2 FOR ORGANIZATIONAL STRUCTURE AND REPORTING PROCESSES USED TO COORDINATE AND EXECUTE SEAT ROLLOUT HAS BEEN MODIFIED AT THE SITE LEVEL. THE FOLLOWING EXECUTION ORDER DESCRIBES THESE IMPROVEMENTS.
4. EXECUTION. ACTION ADDEES ARE CHARGED ICW ISF AND NAVY NMCI PM TO ROLLOUT NMCI FOR THEIR COMMANDS AS SEQUENCED BELOW. THE FOLLOWING ORGANIZATIONAL AND REPORTING REQUIREMENTS PERTAIN.
A. SITE LEADERSHIP. ECHELON 2 COMMANDERS SHALL DESIGNATE A COMMANDER AND A SITE LEAD FOR THE NMCI ROLLOUT FOR THEIR SITES. POC INFO SHALL BE PROVIDED TO DIRECTOR NMCI, INFO NAVY NMCI PM. USING AN OPERATIONAL ANALOGY, THE DIRECTOR NMCI FUNCTIONS AS THE OSE (OFFICER SCHEDULING THE EVENT), THE ECHELON 2 AS THE OCE (OFFICER CONDUCTING THE EVENT), AND THE SITE COMMANDER AS THE OTC (OFFICER IN TACTICAL CONTROL). THE COMMAND'S SITE LEADER SUPPORTS THE OTC AND RESPONSIBILITIES INCLUDE:
(1) SERVE AS A MEMBER OF NMCI SITE ROLLOUT LEADERSHIP TEAM. THE TEAM CONSISTS OF THE SITE INTEGRATION LEADER (SIL) FROM THE NAVY NMCI PM, THE VENDOR LEAD, AND THE COMMAND SITE LEADER (CSL). THE VENDOR LEAD IS FROM THE INFORMATION STRIKE FORCE (ISF). THE SIL LEADS THE NMCI SITE ROLLOUT LEADERSHIP TEAM, FUNCTIONING SIMILARLY TO A SHIP'S SUPERINTENDENT IN THE SHIPYARD REPAIR BUSINESS. THE SITE ROLLOUT LEADERSHIP TEAM WILL MAKE ALL TACTICAL DECISIONS REGARDING SITE ROLLOUT, LOCAL SCHEDULE DATES, PRIORITIES, AND ASSIGNMENT OF RESOURCES. WHEN NEEDED, THE ESCALATION OF SITE ROLLOUT ISSUES AND DECISIONS WILL BE FROM THE SIL TO THE NAVY NMCI PM TO THE DIRECTOR NMCI, AND IF NEEDED TO THE OTC TO THE OCE TO THE OSE.
(2) ACT AS THE SINGLE AUTHORITATIVE REPRESENTATIVE FOR ALL NMCI USERS AT A SITE DURING ROLLOUT.
(3) DIRECT, COORDINATE, AND REPORT STATUS ON THE EXECUTION OF COMMAND SITE TASKS NECESSARY TO SUPPORT SITE ROLLOUT. THE DETAILS

OF THESE TASKS, INCLUDING VENDOR REQUIRED ACTIONS, CAN BE FOUND IN THE NMCI EXECUTION PLAN, AOR AND CUTOVER CHECKLISTS, AND OTHER DOCUMENTS THAT CAN BE ACCESSED AT THE NAVY NMCI PM WEBSITE HTTPS:/NMCI.SPAWAR.NAVY.MIL/ OR THE VENDOR NMCI WEBSITE AT WWW.EDS.COM/NMCI/TRANSITION.HTM. SPECIFIC REPORTING PROCEDURES TO BE PROVIDED UNDER SEPCOR.
B. AT THOSE SITES WHERE THERE ARE ORGANIZATIONS FROM MULTIPLE ECHELON 2 COMMANDS, A LEAD ECHELON 2 IS DESIGNATED BY DIRECTOR NMCI (PARA 5). THE LEAD ECHELON 2 WILL BE RESPONSIBLE FOR SELECTING THE SITE COMMANDER AND THE COMMAND SITE LEADER PER PARA 4A.
5. SEQUENCING PLAN: FOLLOWING SITES ARE DIRECTED FOR CUTOVER IN THIRD QUARTER FY02 (SEAT OBJECTIVES ARE MINIMUMS):
A. NAS LEMOORE
(1) LEAD ECHELON 2: CINCPACFLT
(2) OTHER ECHELON 2(S): RESFOR
(3) CUTOVER START: 22 OCT 01
(4) CUTOVER FINISH: 07 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 3000 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. DOUG FRIDLUND, EMAIL FRIDLUND@SPAWAR.NAVY.MIL, 619-524-7481, CEL 619-559-1149
B. NAS PATUXENT RIVER
(1) LEAD ECHELON 2: NAVAIR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 13 MAR 02
(4) CUTOVER FINISH: 30 OCT 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 3800 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. STAN WICHOWSKI, EMAIL STANW@SPAWAR.NAVY.MIL,619-204-6048
C. NSWC DIV PORT HUENEME
(1) LEAD ECHELON 2: NAVSEA
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 15 MAY 02
(4) CUTOVER FINISH: 04 SEP 02
(5) SEAT OBJECTIVE BY 26 JUL 02: 2453 SEATS
(6) PMO SITE INTEGRATION LEAD: CDR BRION TYLER, EMAIL TYLERB@SPAWAR.NAVY.MIL, 858-537-0312, CEL 619-804-3236
D. SPAWARSYSCOM HQ
(1) LEAD ECHELON 2: SPAWAR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 20 MAY 02
(4) CUTOVER FINISH: 27 SEP 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 1562 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. DINGUS GAYHEART, EMAIL GAYHEART@SPAWAR.NAVY.MIL, 619-524-7972, CEL 619-204-3853
E. CRYSTAL CITY
(1) LEAD ECHELON 2: CNO
(2) OTHER ECHELON 2(S): AAUSN, SPAWAR, NAVAIR
(3) CUTOVER START: 29 MAY 02
(4) CUTOVER FINISH: 09 OCT 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 876 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. BOB COONEY, EMAIL COONEY@SPAWAR.NAVY.MIL, 703-989-4437
F. PENTAGON
(1) LEAD ECHELON 2: AAUSN
(2) OTHER ECHELON 2(S): CNO
(3) CUTOVER START: 29 MAY 02
(4) CUTOVER FINISH: 06 DEC 02

(5) SEAT OBJECTIVE BY 30 JUN 02: 832 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. BOB COONEY, EMAIL
COONEY@SPAWAR.NAVY.MIL, 703-989-4437
G. CINCLANTFLT HQ
(1) LEAD ECHELON 2: CLF
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 10 JUN 02
(4) CUTOVER FINISH: 14 JUN 02
MSGID/GENADMIN/PEO-IT WASHINGTON DC/0008//
SUBJ/NMCI 20K ROLLOUT EXECUTION ORDER//
(5) SEAT OBJECTIVE BY 30 JUN 02: 1350 SEATS
(6) PMO SITE INTEGRATION LEAD: MS. KATHY OCHOA, EMAIL
KOCHOA@SPAWAR.NAVY.MIL, 757-558-6825, CEL 757-617-7473
H. WASHINGTON NAVY YARD
(1) LEAD ECHELON 2: NDW
(2) OTHER ECHELON 2(S): AAUSN, CNO, NNOC
(3) CUTOVER START: 03 JUN 02
(4) CUTOVER FINISH: 24 OCT 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 1083 SEATS
(6) PMO SITE INTEGRATION LEAD: CAPT(SEL) DAN DEATLEY, EMAIL
DEATLEY@SPAWAR.NAVY.MIL, 858-537-0312, CEL 619-301-1487
I. NRC NEW ORLEANS
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 03 JUN 02
(4) CUTOVER FINISH: 07 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 114 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL
ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603, CEL 858-705-2785
J. NAS ATLANTA
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 03 JUN 02
(4) CUTOVER FINISH: 27 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 663 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. MICHAEL LAHMAN, EMAIL
LAHMAN@SPAWAR.NAVY.MIL, 858-537-8551
K. NRC BATON ROUGE
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 10 JUN 02
(4) CUTOVER FINISH: 12 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 38 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL
ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
L. REDCOM SOUTH HQ
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 17 JUN 02
(4) CUTOVER FINISH: 24 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 77 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL
ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
M. NAS FALLON
(1) LEAD ECHELON 2: CPF
(2) OTHER ECHELON 2(S): CNO
(3) CUTOVER START: 10 JUN 02

(4) CUTOVER FINISH 02 AUG 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 800 SEATS
(6) PMO SITE INTEGRATION LEAD: LCDR RANDY BURCHAK, EMAIL BURCHAKA@SPAWAR.NAVY.MIL, 619-524-7606
N. NDW NEBRASKA AVE COMPLEX
(1) LEAD ECHELON 2: NNOC
(2) OTHER ECHELON 2(S): AAUSN, CNO, NDW
(3) CUTOVER START: 10 JUN 02
(4) CUTOVER FINISH: 01 OCT 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 749 SEATS
(6) PMO SITE INTEGRATION LEAD: CAPT(SEL) DAN DEATLEY, EMAIL DEATLEY@SPAWAR.NAVY.MIL, 858-537-0312, CEL 619-301-1487
O. NAWC TSD ORLANDO
(1) LEAD ECHELON 2: NAVAIR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 11 JUN 02
(4) CUTOVER FINISH: 11 JUL 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 1200 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. STAN WICHOWSKI, EMAIL STANW@SPAWAR.NAVY.MIL, 619-204-6048
P. NRC FORT WORTH
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 17 JUN 02
(4) CUTOVER FINISH: 24 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 164 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
Q. NSWC CRANE
(1) LEAD ECHELON 2: NAVSEA
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 12 JUN 02
(4) CUTOVER FINISH: 03 JAN 03
(5) SEAT OBJECTIVE BY 30 JUN 02: 1000 SEATS
(6) PMO SITE INTEGRATION LEAD: CDR CRAIG GOODMAN, EMAIL CGOODMAN@SPAWAR.NAVY.MIL, 858-537-0312, CEL 619-804-3218
R. NAR POINT MUGU
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 17 JUN 02
(4) CUTOVER FINISH: 26 AUG 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 307 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. ROBERT CRUZ, EMAIL CRUZRP@SPAWAR.NAVY.MIL, 619-524-7606
S. NDW ANACOSTIA ANNEX
(1) LEAD ECHELON 2: NDW
(2) OTHER ECHELON 2(S): FSA (CNO)
(3) CUTOVER START: 24 JUN 02
(4) CUTOVER FINISH: 28 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 276 SEATS
(6) PMO SITE INTEGRATION LEAD: CAPT(SEL) DAN DEATLEY, EMAIL DEATLEY@SPAWAR.NAVY.MIL, 858-537-0312, CEL 619-301-1487
T. NRC SHREVEPORT
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 24 JUN 02
(4) CUTOVER FINISH: 28 JUN 02

(5) SEAT OBJECTIVE BY 30 JUN 02: 65 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
U. NRC LUBBOCK
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
MSGID/GENADMIN/PEO-IT WASHINGTON DC/0008//
SUBJ/NMCI 20K ROLLOUT EXECUTION ORDER//
(3) CUTOVER START: 24 JUN 02
(4) CUTOVER FINISH: 28 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 34 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
V. NRC SAN ANTONIO
(1) LEAD ECHELON 2: RESFOR
(2)OTHER ECHELON 2(S): NA
(3) CUTOVER START: 24 JUN 02
(4) CUTOVER FINISH: 28 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 42 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
W. NRC AMARILLO
(1) LEAD ECHELON 2: RESFOR
(2) OTHER ECHELON 2(S): NA
(3) CUTOVER START: 24 JUN 02
(4) CUTOVER FINISH: 28 JUN 02
(5) SEAT OBJECTIVE BY 30 JUN 02: 28 SEATS
(6) PMO SITE INTEGRATION LEAD: MR. JOHN ZAREM, EMAIL ZAREMJ@SPAWAR.NAVY.MIL, 619-524-7603
6. NMCI ROLLOUT IS A DEPARTMENT OF THE NAVY ENTERPRISE ENDEAVOR. AS SUCH, NMCI ROLLOUT IS A TASK THAT EACH SITE MUST COMPLETE WHEN THEY ARE SEQUENCED. HENCE, THE GOALS AND SUCCESS OF THE ENTERPRISE AS A WHOLE (SECURITY, OPERATIONS, AND INTEROPERABILITY) NECESSARILY TAKE PRECEDENCE OVER INDIVIDUAL DESIRES. THE TRANSITION PROCESS ASSOCIATED WITH NMCI ROLLOUT WILL BY ITS NATURE PRESENT SOME SHORT TERM RISKS. OUR PHILOSOPHY IS TO MITIGATE THIS RISK NOT AVOID IT.
A. SUCCESSFUL ENTERPRISE ROLLOUT REQUIRES SIGNIFICANT COORDINATION ACROSS MANY SITES. CONSEQUENTLY, ONCE AOR/CUTOVER ARE SET IN MOTION, ANY RESCHEDULING (STARTING, STOPPING, REPHASING) MUST BE DONE ICW ALCON. WORK STOPAGES OR HOLDS WILL ONLY BE ALLOWED IF AUTHORIZED BY DIRECTOR NMCI OR THE NMCI PM'S FROM NAVY OR USMC.
B. THE SITE CSL WILL BE AN ESSENTIAL ELEMENT WITHIN THE NMCI ROLLOUT TEAM. SUCCESS OF THIS MISSION WILL DEMAND THE SUPPORT OF THE ENTIRE COMMAND. COORDINATION AND CONSTANT COMMUNICATIONS, BOTH VERTICALLY AND HORIZONTALLY THROUGHOUT THE PROCESS, WILL BE THE KEY.
7. RADM MUNNS, DIRECTOR NMCI, SENDS.//
BT
#0003
NNNN

D9. 211601Z MAR 03

Subject: NMCI - SUMMER 2003 SCHEDULE RESTRUCTURING

PRIORITY

P 211601Z MAR 03 PSN 265646S29

MSGID/GENADMIN/PEO IT WASHINGTON DC NMCI/0026/MAR//

SUBJ/NMCI - SUMMER 2003 SCHEDULE RESTRUCTURING//

REF/A/VTC/DIRECTOR NMCI WASHINGTON DC/13MAR2003//

REF/B/CON/DIRECTOR NMCI WASHINGTON DC/18MAR2003//

REF/C/CON/DIRECTOR NMCI WASHINGTON DC/19MAR2003//

REF/D/DOC/PEO IT WASHINGTON DC/06OCT2000//

NARR/REF A IS VTC CHAIRED BY DIR NMCI, ISF AND PMO.

REF B IS THE OPS ADVISORY BOARD (OAB) ON 18 MAR 2003. REF C IS THE DIR NMCI-ASNRDA MEETING ON 19 MAR 2003. REF D IS THE NMCI CONTRACT.// POC/CRAIG MADSEN/CAPT PMW164/COMSPAWARSYSCOM/-/TEL:(619)524-7604 /EMAIL:CRAIG.MADSEN@NAVY.MIL// POC/RICH GLOVER/CIV/MARCORPSYSCOM/-/TEL:(703)784-0709 /EMAIL:GLOVERRA@MCSC.USMC.MIL// POC/JOSEPH SPITEK/CAPT SEL/DIR NMCI/-/TEL:(703)685-5519 /EMAIL:JOSEPH.SPITEK1@NAVY.MIL// POC/JOSEPH SPRUILL/CDR/DIR NMCI/-/TEL:(703)685-5524 /EMAIL:JOSEPH.SPRUILL@NAVY.MIL// POC/DEBBIE STREUFERT/CIV/DIR NMCI/-/TEL:(703)685-5508 /EMAIL:DEBBIE.STREUFERT@NAVY.MIL//

RMKS/1. REFS A THROUGH C, DISCUSSED CRITERIA FOR ASSUMPTION OF RESPONSIBILITY (AOR) FOR NMCI SERVICES, SCHEDULE SLIPPAGE IN JAN/FEB AND THE POTENTIAL ACCELERATION OF AORS FOR BOTH THE NAVY AND MARINE CORPS TO 01 MAY 2003. NEW PROCEDURES AND SCHEDULE REALIGNMENT WERE DISCUSSED AT THE OAB, REF B, AND ARE SUMMARIZED BELOW.

2. AOR CRITERIA CHANGES. THE FOLLOWING FIVE ITEMS ARE THE DIRECTOR NMCI CRITERIA FOR BEGINNING AOR. EACH OF THE ITEMS SHALL BE COMPLETED NO LATER THAN THE TIME LINE RECOMMENDATION CONTAINED BELOW:

APPROVED ORDER. THE FINAL ORDER MUST BE SUBMITTED VIA NOIS/EMARKETPLACE WITH FUNDING AND AWARDED BY THE ACO 30 DAYS PRIOR TO AOR. THE AOR DATE WILL BE ENTERED AS THE START DATE.

PRELIMINARY SITE QUESTIONNAIRE (PSQ) (PARTIAL). SECTION 2 ITEM 2.4 (SITE INFORMATION, TRANSITION TEAM POCS), SECTION 5 (BASE SECURITY INFORMATION), AND SECTION 8 (INCUMBENT CONTRACTORS) OF THE PSQ MUST BE SUBMITTED 30 DAYS PRIOR TO AOR. THESE SECTIONS ALLOW EDS TO START THE LONGER LEAD TIME PERSONNEL ACTIONS ASSOCIATED WITH AOR. THE PSQ CAN BE DOWNLOADED FROM <HTTP:/WWW.NMCI.NAVY.MIL/PRIMARY_AREAS/TRANSITION_TO_NMCI/PHASE_1_PRE_AOR_PLANNING_PHASE>.

PSQ (FULL) AND SITE CONCURRENCE MEMORANDUM (SCM). FULL PSQ SUBMITTED TO EDS. SCM COMPLETED TO INCLUDE SEATS, LEASES, AND SHARED INFRASTRUCTURE. DUE DATE - 10 DAYS PRIOR TO AOR.

ISF ASSUMES IT SUPPORT. SUFFICIENT EDS PERSONNEL ARE ON SITE TO ASSUME IT INFRASTRUCTURE OPERATIONS AND MAINTENANCE. DUE DATE -DATE IN ORDER SHOWN AS START OF AOR.

IMPACTED PERSONNEL. SINCE PERSONEL MAKE INDIVIDUAL DECISIONS, THIS ITEM MAY RUN THROUGH AOR START PROVIDING EDS HAS SUFFICIENT PERSONNEL ON SITE TO ASSUME THE LEGACY NETWORK AS OF THE AOR DATE. COMPLETION OF IMPACTED PERSONNEL INCLUDING EDS JOB OFFERS MUST BE COMPLETED NO LATER THAN 30 DAYS AFTER AOR.

3. **ACCELERATION OF AOR FOR NAVY AND MARINE CORPS SEATS TO 01 MAY 2003. SITES WITH AOR DATES SCHEDULED TO START AFTER 01 MAY 2003 ARE DIRECTED TO ACCELERATE TO 1 MAY 2003** AS DISCUSSED WITH CLAIMANTS DURING DIRECTOR NMCI SCHEDULER CONFERENCE CALLS. THIS WILL IMPACT BOTH NAVY AND MARINE CORPS SEATS AND WILL BE LIMITED BY CONGRESSIONAL AUTHORIZATIONS, ONE OF WHICH LIMITS TOTAL ORDERS TO 310,000 SEATS. THIS WILL BE DONE WITHIN CURRENT DON NMCI BUDGET AND WILL IMPACT ABOUT 20,000 NAVY SEATS. USMC IMPACT IS TBD.BENEFITS TO ACCELERATION OF AOR INCLUDE:

ALLOWS NMCI DAA (CNNWC) GREATER LATITUDE AND EFFICIENCY IN CORRECTING IA ISSUES ASSOCIATED WITH THE TRANSITION OF LEGACY NETWORKS TO NMCI.
BY PROVIDING AN EXPANDED POPULATION EDS MAY BETTER LEVERAGE COMMERCIAL SECTOR EXPERTISE TO IMPROVED THE EFFICIENCY OF THE NMCI TRANSITION, AND THE QUALITY OF CUTOVER SEATS.
RESTRUCTURES THE REMAINING FY03 SCHEDULE TO ALLOW THE DON TO ACHIEVE CONTRACT MINIMUMS. WE ARE TAKING A NUMBER OF ACTIONS TO ENSURE THESE ACCELERATED AORS DO NOT LEAD TO AN EXTENDED TIME FROM AOR TO THE ROLLOUT OF SEATS. IN ADDITION TO MANAGING REASONABLE TRANSITION TIMES, THE PMO, NMCI DIRECTOR?S STAFF AND EDS ARE WORKING JOINTLY TO DEVELOP SPECIFIC SERVICE LEVEL AGREEMENTS (SLA) TO MANAGE THE AOR PERIOD. IN GENERAL, THE SLA WILL COVER SECURITY/IAVA COMPLIANCE, MAINTENANCE OF SYSTEM PERFORMANCE, AND LIMITED IT MODERNIZATION.

4. MODIFICATION OF ORDERS. CLAIMANTS WITH SITES HAVING AOR DATES AFTER 1 MAY 2003 ARE DIRECTED TO MODIFY ORDERS TO REFLECT 1 MAY 2003 START DATE. SPECIFIC DETAILS ON SITES AND FUNDING TO BE SENT SEPCOR.

5. ALCON WILL CONTINUE TO REFINE PROCESSES AS SEAT ROLLOUT CONTINUES. YOUR CONTINUED INVOLVEMENT AND COMMENTS ARE BOTH SPECIFICALLY REQUESTED AND APPRECIATED. ANY QUESTIONS CAN BE DIRECTED TO THE ABOVE LISTED POCS WITH RESPONSIBILITIES AS FOLLOWS: CAPT CRAIG MADSEN: NAVY AOR CRITERIA CHANGES, SCHEDULE IMPLICATIONS, AND NAVY PROGRAM MANAGEMENT ISSUES. RICH GLOVER: USMC AOR CRITERIA CHANGES, SCHEDULE IMPLICATIONS, AND USMC PROGRAM MANAGEMENT ISSUES. CAPT (SEL) JOE SPITEK: ORDER AND SCHEDULE MODIFICATIONS CDR JOE SPRUILL: FUNDING ISSUES DEBBIE STREUFERT: NMCI PCO

6. MINIMIZE CONSIDERED. RELEASED BY RADM CHARLES L. MUNNS.//

BT
#0026
NNNN

D10. 242225Z MAY 02

SUBJ/NMCI PROCESS SUMMIT AGREEMENTS//

R 242225Z MAY 02 COMSPAWARSYSCOM SAN DIEGO CA NMCI PROCESS SUMMIT AGREEMENTS//
CORRECTED COPY ATTENTION INVITED TO
ADMINISTRATIVE MESSAGE
ROUTINE
UNCLAS //N2060//
MSGID/GENADMIN/COMSPAWARSYSCOM/PMW164//
SUBJ/NMCI PROCESS SUMMIT AGREEMENTS//
REF/A/GENADMIN/PEO IT WASHINGTON DC/202304ZMAY2002//
AMPN/REF A IS NMCI 20K ROLLOUT EXECUTION ORDER.//
POC/ROBERT LOGAN/COL/NMCI DEPUTY DIRECTOR/-/TEL:CML:(703)685-5510
/EMAIL:RLOGAN'AT'SPAWAR.NAVY.MIL//
POC/CRAIG MADSEN/CAPT/NAVY NMCI PM/-/TEL:619-524-7553
/EMAIL:MADSENC'AT'SPAWAR.NAVY.MIL//
POC/RICH GLOVER/CIV/PM USMC NMCI/-/TEL:DSN: 278-0709
/EMAIL: GOVERRA'AT'MCSC.USMC.MIL//
POC/TIM TRAVERSO/CIV/NADTF-NAVY CIO/-/TEL:703-602-5995
/EMAIL: TRAVERSO.TIMOTHY'AT'HQ.NAVY.MIL//
RMKS/1. THIS IS A COORDINATED NAVAL MESSAGE FROM DIRECTOR NMCI, NAVY AND MARINE CORPS PROGRAM OFFICES, AND THE NMCI ISF. ON MAY 7 - 9, REPRESENTATIVES FROM THESE ORGANIZATIONS HELD A SUMMIT TO DISCUSS AND DEFINE PROCESSES TO IMPROVE AND ACCELERATE NEAR TERM NMCI SEAT ROLLOUT. THIS NAVAL MESSAGE SUMMARIZES THE AGREEMENTS REACHED ON THESE PROCESSES.
2. BACKGROUND. FUTURE NMCI CUSTOMERS HAVE SEEN A VARIETY OF PROCESS DOCUMENTS, HAVE ATTENDED VARIOUS NMCI FORUMS, OR HAVE HAD THE OPPORTUNITY TO OBSERVE THE EARLY NMCI INSTALLATION EFFORTS. TO DATE, NMCI SEAT ROLLOUT HAS BEEN SLOWER THAN EXPECTED OR DESIRED. THROUGH A COMBINED EFFORT AT THE NMCI PROCESS SUMMIT, HIGH LEVERAGE ITEMS WERE IDENTIFIED RELATED TO LEGACY APPLICATIONS AND INFORMATION ASSURANCE. ALSO, RELATED NMCI TRANSITION ISSUES WERE IDENTIFIED AND PRIORITIZED.
3. PROCESS CHANGES. THE DIRECTOR NMCI AUTHORIZES THE PROCESSES SUMMARIZED BELOW FOR IMMEDIATE IMPLEMENTATION AT SITES TRANSITIONING TO NMCI IN ACCORDANCE WITH REF A. SPECIFIC PROCESS DETAILS WILL BE PROVIDED SEPCOR, BUT THE SIGNIFICANT CHANGES ARE SUMMARIZED BELOW. A. LEGACY APPLICATIONS:
(1) LOCAL APPLICATION LOADING (EITHER MANUALLY OR THROUGH AN IMAGE BUILD) IS APPROVED. APPLICATIONS SUITABLE FOR LOCAL LOADING MUST BE ON THE SITE'S RATIONALIZED LIST.
(2) USER TO APPLICATION MAPPING WILL BE REQUIRED AT THE TIME FINAL RATIONALIZED LISTS ARE DUE (AOR-60 DAYS).
(3) REVISE LEGACY APPLICATION PROCESSES TO SHORTEN TIMELINE BY APPLYING APPLICATION "FUNNELING" PROCESSES AND EMPOWERING THE NADTF TO APPLY APPLICATION RULE SETS TO REDUCE RATIONALIZED LISTS. ON-SITE LEADERSHIP WILL EXPLAIN THE FUNNELING PROCESS IN DETAIL. ITS PURPOSE IS TO QUICKLY SORT AND PRIORITIZE EXISTING LEGACY APPLICATIONS.
(4) THE LEGACY APPLICATION MIGRATION RULE SET (LED BY NADTF) INCLUDES THE FOLLOWING:
(A) WINDOWS 2000 COMPLIANT APPLICATIONS ONLY
(B) COMPLIANT WITH DON/DOD SECURITY POLICY

(C) NO PERSONAL, NON-MISSION, OR NON-BUSINESS-RELATED SOFTWARE
(D) NO GAMES
(E) NO FREEWARE OR SHAREWARE
(F) NO BETA OR TEST VERSION SOFTWARE PACKAGES
(G) NO APPLICATION DEVELOPMENT SOFTWARE (EXCEPTION APPLIES FOR APPROVED SCIENCE AND TECHNOLOGY [S AND T] SEATS)
(H) NO AGENTS
(I) NO DUPLICATION OF STANDARD SEAT SERVICES
(J) NO 8 OR 16 BIT APPLICATIONS
(5) ALL MEDIA NEEDS TO BE HELD ONSITE AND SUBMITTED TO THE ISF. CONTINUE TO USE THE ISF TOOLS DB TO CREATE REQUEST FOR SERVICE (RFS) FOR ALL LEGACY APPLICATIONS REQUIREMENTS.
(6) IA VULNERABILITY ASSESSMENT PACKAGES WILL BE DEVELOPED AND PROVIDED POST SEAT CUTOVER VICE PRIOR TO SEAT CUTOVER.
(7) APPLICATIONS WILL BE TESTED USING A PIAB, A LADRA TEST SEAT, OR THE ISF CERTIFICATION LAB IN SAN DIEGO. ISF WILL DETERMINE MEANS AND LOCATION OF TESTING.
(8) APPLICATIONS THAT SUCCESSFULLY PASS NMCI CERTIFICATION AND B1/B2 TESTING WILL BE AUTHORIZED FOR OPERATION ON NMCI.
(9) ISF WILL GENERATE A WEEKLY REPORT FOR DELIVERY TO THE NMCI DAA. THE WEEKLY REPORT WILL PROVIDE INFORMATION PERTAINING TO APPLICATION INSTALLATION METHOD, TESTING RESULTS, AND NUMBER OF SEATS INSTALLED FOR EACH SITE.
(10) APPLICATIONS THAT FAIL CERTIFICATION AND/OR B1/B2 TESTING WILL BE QUARANTINED ON THE LEGACY NETWORK.
(11) APPLICATIONS THAT ARE IDENTIFIED OR SUBMITTED LATE AND SUBSEQUENTLY APPROVED BY NADTF WILL BE QUARANTINED ON THE LEGACY NETWORK. IF DISAPPROVED BY NADTF, APPLICATION(S) WILL NOT BE SUPPORTED BY NMCI. B. INFORMATION ASSURANCE: THE FOLLOWING ISSUES HAVE RECEIVED PROGRAM ENDORSEMENT AND HAVE BEEN FORWARDED TO THE NMCI DAA FOR APPROVAL.
(1) SHORTEN TIMELINE TO ACHIEVE SITE IATO FROM 31 DAYS TO 24 DAYS INCLUDING 8 DAYS FOR FORMAL DAA REVIEW AND APPROVAL. DAA TO ASSIGN DELEGATE AUTHORITY TO ASSIST IN OVERCOMING DAA AVAILABILITY. ISF/PMO TO PROVIDE DAA 24-72 HOUR NOTICE OF UPCOMING CRITICAL DECISION MILESTONES.
(2) IATO/IATC IN PARALLEL. GOVERNMENT APPROVAL TO LAUNCH APPLICATIONS TO TEST SEATS ON THE OPERATIONAL NETWORK FOR TESTING. APPROVAL EXTENDS TO APPLICATIONS AND SEATS USED FOR NMCI SECURITY/GPO TESTING ONLY. APPLICATIONS INCLUDE ONLY THOSE CURRENTLY RUNNING IN LEGACY ENVIRONMENT.
(3) ON COMPLETION OF BOUNDARY 2 BUILD AND SCAN, DAA TO APPROVE, IN PHONECON OR EMAIL VICE LETTER, CONNECTION TO NETWORK.
(4) ON COMPLETION OF SERVER FARM BUILD AND SCAN, DAA TO APPROVE, IN PHONE CON OR EMAIL VICE LETTER, APPROVAL TO CONNECT TO BOUNDARY.
4. WORKING ISSUES. IN ADDITION TO THE LEGACY APPLICATION AND INFORMATION ASSURANCE PROCESS CHANGES OUTLINED ABOVE, WORK CONTINUES ON COMMAND AND CONTROL AT SITES, THE ROLLOUT SCHEDULE BEYOND THE FIRST 20K SEATS, AN ENTERPRISE POLICY/PLAN TO BASELINE THE KIOSK PROCESS, AND THE USER TO APP MAPPING PROCESS. APPROXIMATELY 50 TRANSITION ISSUES WERE IDENTIFIED AS HAVING THE POTENTIAL TO DIRECTLY EFFECT RAPID SEAT ROLLOUT AND WILL ALSO CONTINUE TO BE WORKED. EXAMPLES OF THESE ISSUES INCLUDE MACS, S AND T CLIN 0038, LEGACY DEVICE SUPPORT, AND END USER AVAILABILITY.
5. THE NMCI DIRECTOR'S OFFICE, NAVY AND MARINE CORPS PROGRAM OFFICES, AND THE ISF WILL CONTINUE TO REFINE PROCESSES TO INCORPORATE LESSONS LEARNED AS SEAT ROLLOUT CONTINUES. YOUR

```
CONTINUED INVOLVEMENT AND COMMENTS ARE BOTH SPECIFICALLY
REQUESTED AND APPRECIATED.//
BT
#5462
NNNN
```

D11. 152000Z MAY 03

Subject: NMCI CONTINUING GUIDANCE-TRANSITION MSG NO. A002

Importance: Low

R 152000Z MAY 03 CMC WASHINGTON DC

ATTENTION INVITED TO

ROUTINE

UNCLAS

THIS IS A 2 SECTION MESSAGE COLLATED BY DMDS

QQQQ

SUBJ: NMCI CONTINUING GUIDANCE-TRANSITION MSG NO. A002
UNCLASSIFIED//
MARADMIN 236/03

MSGID/GENADMIN/CMC WASHINGTON DC/C4//

SUBJ/NMCI CONTINUING GUIDANCE-TRANSITION MSG NO. A002//

REF/A/MSG/CMC WASHINGTON DC C4/161210ZJAN2003/MARADMIN/-/-//

REF/B/MSG/MARFORPAC/230148ZAPR2003/-/NOTAL/-//
POC/S.L. CABRIAN/CIV/HQMC C4 CP/-/TEL:DSN 223-3490/TEL:703-693-3490
/EMAIL:CABRIANSL@HQMC.USMC.MIL//

NARR/REF A IS INITIAL NMCI WARNING ORDER MARADMIN 019/03. REF B IS
A COORDINATED MARFORPAC, MARFORLANT MESSAGE THAT PROPOSES AN
ALTERNATE NMCI TRANSITION PLAN FOR MARINE AVIATION UNITS.//
GENTEXT/REMARKS/1. THE MARINE CORPS HAS BEEN ANTICIPATING THE
ARRIVAL OF NMCI FOR OVER TWO YEARS. ELECTRONIC DATA SYSTEMS
CORPORATION (EDS) HAS ASSUMED RESPONSIBILITY (AOR) FOR THE FIRST
11,000 OF APPROXIMATELY 89,000 MARINE CORPS USERS AT QUANTICO VA,
THE NATIONAL CAPITOL REGION (NCR), MARFORRES HEADQUARTERS NEW
ORLEANS, AND MCLB ALBANY. AORS WILL CONTINUE THROUGHOUT FY03 AND
INTO FY04. WHILE WE ARE STILL WORKING TO DETERMINE THE OVERALL COST
OF NMCI TO THE MARINE CORPS, WE DO KNOW THAT DEMAND FOR NMCI-LIKE
SERVICES HAS INCREASED SIGNIFICANTLY POST 9/11 GIVEN A BETTER
UNDERSTANDING OF THE CONTRACT. THE MARINE CORPS REMAINS COMMITTED
TO THE OVERALL GOAL OF A SINGLE DON ENTERPRISE NETWORK AND TO NMCI
AS A MEANS TO ACHIEVE THAT GOAL. ALSO, ACCURATELY PLANNING AND
SUPPORTING THE TRANSITION OF FORCES SUPPORTING OPERATION ENDURING
FREEDOM, IRAQI FREEDOM, AND THE GLOBAL WAR ON TERRORISM REMAINS A
PRIORITY. WE ARE WORKING HARD TO AVOID ACTIONS THAT NEGATIVELY
IMPACT READINESS, AND ARE WORKING CLOSELY WITH THE DIRECTOR NMCI
AND HIS STAFF ON THE VARIOUS CHALLENGES ASSOCIATED WITH
TRANSITIONING THE MARINE CORPS AND THE NAVY TO NMCI. TO
OPERATIONALIZE THE TRANSITION PROCESS, WE HAVE INCORPORATED THE
MITNOC INTO THE OVERALL PROCESS AS A KEY ENABLER AND TO LEVERAGE
THEIR ENTERPRISE TECHNICAL EXPERTISE.

2. THIS MSG BUILDS ON REF A AND PROVIDES ADDITIONAL GUIDANCE RELATED TO NMCI TRANSITION AND IMPLEMENTATION. TO ASSIST COMMANDERS, THE AOR SCHEDULE AND CURRENT TRANSITION STATUS FOR THE MARINE CORPS CAN BE FOUND AT HTTPS:(DOUBLE_SLASH)WWW.NMCIINFO.USMC.MIL. ADDITIONAL GUIDANCE PERTINENT TO MARINE CORPS SITES SCHEDULED FOR TRANSITION IS CONTAINED BELOW.

3. COMMAND RESPONSIBILITIES. WHILE WE ARE COMMITTED TO MEETING THE AOR SCHEDULE, OUR GOAL IS TO TRANSITION SMARTLY. THIS REQUIRES THE ACTIVE PARTICIPATION OF COMMANDERS' TO ENSURE COMMAND NMCI ORDERS ARE ACCURATE, VALIDATED, AND SUBMITTED IN A TIMELY MANNER. ADDITIONALLY, COMMAND SITE REPRESENTATIVES MUST WORK WITH MCSC AND EDS TO ACCOMPLISH THE OTHER CRITICAL ACTIVITIES IN THE PRE-AOR CHECKLIST LISTED ON THE MARINE CORPS NMCI INFORMATION WEB PAGE AT HTTPS:(DOUBLE_SLASH)WWW.NMCIINFO.USMC.MIL. PARTICULAR ITEMS OF IMPORTANCE THAT COMMANDERS SHOULD PAY PARTICULAR ATTENTION TO INCLUDE:
A. WHETHER SEAT ORDERS ARE COMPLETE;
B. WHAT THE STATUS IS OF THE PRELIMINARY SITE QUESTIONNAIRE;
C. WHETHER A SITE CONCURRENCE MEMO HAS BEEN EXECUTED;
D. IDENTIFICATION OF IMPACTED PERSONNEL BY NMCI; AND
E. ACTIONS TAKEN TO PLACE IN NEW JOBS.

4. ORGANIZING FOR TRANSITION. THE COMMAND SITE REPRESENTATIVES COMBINED WITH THE MCSC PM-NMCI (REGIONAL) CONTRACTING OFFICER REPRESENTATIVES (CORS/RCORS) HAVE BEEN CREATED TO MEET THE CHALLENGES OF MEETING USER NEEDS WHILE EXECUTING A SMOOTH TRANSITION. 16 RCORS HAVE BEEN PROVISIONED TO SUPPORT THE USMC NMCI TRANSITION. THEIR DUTIES INCLUDE HELPING LOCAL PERSONNEL TO UNDERSTAND THE CONTRACT AND MAKE THE BEST SERVICE CHOICES POSSIBLE. THE RCORS WILL ASSIST LOCAL CUSTOMER TECHNICAL REPRESENTATIVES (CTRS) AND COMMAND REPRESENTATIVES WITH TECHNICAL EXPERTISE RELATED TO CONTRACT SERVICES. HQMC P&R HAS FUNDED FOR 61 CTRS IN SUPPORT OF NMCI REQUIREMENTS USMC-WIDE. THESE CTRS WILL WORK WITH G-6/S-6 REPRESENTATIVES AND LOCAL INFORMATION SYSTEMS COORDINATORS (ISCS) TO ENSURE ACCURATE IDENTIFICATION AND ORDERING OF NMCI SEATS AND SERVICES. WE EXPECT THAT ISCS AND G-6 PERSONNEL TO ENLIST THE SUPPORT OF THEIR CTRS IN ANSWERING QUESTIONS CONCERNING SEAT ORDERS AND OR RESOLVING OTHER CONTRACT/SERVICE RELATED ISSUES. AS REQUIRED, CTRS WILL RAISE ISSUES/CONCERNS TO THE RCORS FOR CLARIFICATION AND ANY NECESSARY FOLLOW-ON ACTION. THE CURRENT ISC ROLE WILL ALSO CONTINUE AFTER THE NMCI TRANSITION AND WE ENVISION YOUR CURRENT ISC WILL BE A CRITICAL LINK BETWEEN COMMAND NMCI USERS AND THE CTRS. WE ENCOURAGE USERS TO CONTACT THEIR LOCAL CTRS OR RCORS FOR RESOLUTION OF ISSUES OR ANSWERS TO QUESTIONS BEYOND THE SCOPE OF THE LOCAL ISC. MCTOIC, STOIC, CTR, AND R/COR ROLES, RESPONSIBILITIES AND RELATIONSHIPS ARE DESCRIBED IN MORE DETAIL IN REF A.

5. FUNDING. TO ENSURE WE'RE GETTING MAXIMUM CAPABILITY WITHIN THE EXISTING FUNDING BASELINE, COMMANDERS ARE STRONGLY ENCOURAGED TO REVIEW THEIR REQUIREMENTS IAW AMPLIFYING GUIDANCE CONTAINED IN THIS MESSAGE. ALSO, CURRENTLY THE CIO IS WORKING TO DEVELOP A PROCESS FOR VALIDATING REQUIREMENTS AND THE ORDERING OF NEW SERVICES UNDER A CENTRAL CONSTRUCT. THE COST TO IMPLEMENT NMCI REMAINS A MAJOR

CONCERN. WE NEED THE SUPPORT OF EACH COMMANDER TO ENSURE REQUIREMENTS ARE SCRUBBED PRIOR TO SUBMISSION. THESE TYPES OF MEASURES ALLOW THE COMMANDER TO MAXIMIZE HIS CAPABILITY WITHIN EXISTING RESOURCES. SPECIFIC AREAS TO REVIEW INCLUDE:
A. RECOMMEND ALL COMMANDS' DESKTOP SEAT ORDERS BE BLUE SEATS UNLESS THERE IS A SPECIFIC REQUIREMENT FOR A MORE EXPENSIVE SOLUTION. BLUE SEATS WILL MEET THE COMPUTING REQUIREMENTS FOR THE MAJORITY OF MARINE CORPS NMCI USERS.
B. NO ONE SHOULD BE ALLOCATED MORE THAN ONE SEAT. FOR INDIVIDUALS WHO TRAVEL, RECOMMEND ALLOCATING A PORTABLE SEAT, WITH DOCKING STATION, RATHER THAN A SEPARATE DESKTOP AND PORTABLE.
C. CONVERSELY, COMMANDERS SHOULD CONSIDER ASSIGNING MULTIPLE USERS TO A SEAT WHERE IT MAKES SENSE, PARTICULARLY ON THE CLASSIFIED NETWORK.

6. REMOTE SITES. DIRECTOR NMCI, C4, MCSC PM-NMCI, AND EDS REPS WILL CONTINUE TO WORK TOWARDS FINALIZING THE REMOTE SITE SOLUTION. OUR GOAL IS TO HAVE A MARINE CORPS REMOTE SITE TRANSITION SCHEDULE DEVELOPED AND INTEGRATED WITHIN THE OVERALL MARINE CORPS SITES SCHEDULE BY END OF MAY 03.

7. DISN CIRCUIT COSTS. THE MARINE CORPS POSITION CONTINUES TO BE THAT DISN NMCI CIRCUIT COSTS ARE A DON BILL. CURRENTLY, DISA, EDS
,
AND DIRECTOR NMCI ARE NEGOTIATING CREDIT FOR THESE COSTS WITHIN THE CURRENT SEAT PRICE STRUCTURE.

8. DUAL DESKTOP. OUR GOAL IS TO MINIMIZE AND QUICKLY ELIMINATE THE USE OF NON-COMPLIANT LEGACY APPLICATIONS AND DUAL DESKTOPS. A "DUAL DESKTOP" SCENARIO OCCURS WHEN IT IS NECESSARY TO RUN A NON-COMPLIANT LEGACY APPLICATION ON A SEPARATE WORKSTATION OUTSIDE OF THE NMCI QQQQ
DOMAIN. THIS IS A HIGH RISK SITUATION DUE TO SUSTAINMENT COST AND NETWORK SECURITY CONCERNS. MARADMIN 479/02 CONTAINS THE MARINE CORPS LIST OF APPROVED APPLICATIONS AND HAS DETAILED GUIDANCE ON STEPS TO BE TAKEN TO EFFECTIVELY ASSESS APPLICATIONS, SYSTEMS, AND NETWORKS.

9. BLACKBERRY PERSONAL DIGITAL ASSISTANTS (PDAS). THREE DISTINCT OPTIONS ARE AVAILABLE FOR THESE PDAS UNDER THE NMCI CONTRACT. NOTE: IF OPTION 8A OR 8B (LISTED BELOW) IS CHOSEN, YOU MUST TERMINATE SERVICE WITH YOUR CURRENT SERVICE PROVIDER AND START NMCI PROVIDER SERVICE. THIS PROCESS TAKES ABOUT 10 WORKING DAYS. ALTHOUGH RIM "CRYPTO-BERRIES" ARE NOT CURRENTLY SUPPORTED, EFFORTS ARE UNDERWAY TO INCLUDE THESE DEVICES UNDER THE THREE OPTIONS LISTED BELOW:
A. FULL BLACKBERRY SERVICE (NMCI-PROVIDED HANDHELD DEVICE AND WIRELESS SERVICE) ($153 MONTHLY) INTEGRATES SEAMLESSLY WITH THE NMCI USER'S EXISTING E-MAIL ACCOUNT PROVIDING A WIRELESS EXTENSION OF THEIR NMCI E-MAIL MAILBOX. NATIONWIDE WIRELESS NETWORK SUPPORT IS ONLY PROVIDED TO EXISTING COMMERCIAL INFRASTRUCTURE AND COVERAGE AREAS. FEATURES INCLUDE THE ABILITY TO READ, COMPOSE, FORWARD, REPLY, DELETE OR FILE UNCLASSIFIED MESSAGES USING A SINGLE NMCI E-MAIL ADDRESS AND MAILBOX. SERVICE ONLY SUPPORTS "ENTERPRISE" SERVER E-MAIL REDIRECTION PROVIDED BY NMCI. NO DESKTOP REDIRECTOR FUNCTIONS WILL BE SUPPORTED BY THIS SERVICE. USERS CAN CONTROL WHICH MESSAGES THEY RECEIVE ON THEIR WIRELESS HANDHELD BY SETTING E-MAIL FILTERS THAT MONITOR KEY WORDS AND MESSAGE FIELDS FROM THEIR

NMCI DATA SEAT. THIS SERVICE IS ONLY INTEROPERABLE WITH NMCI-PROVIDED E-MAIL SERVICES AND DOES NOT INCLUDE INTEROPERABILITY WITH OTHER MESSAGING SYSTEMS (E.G. DMS). THIS SERVICE INCORPORATES ADVANCE TRIPLE DES ENCRYPTION TECHNOLOGY TO MEET SECURITY GUIDELINES FOR REMOTE E-MAIL ACCESS FOR ALL INCOMING AND OUTGOING TRANSMISSIONS.
B. HYBRID BLACKBERRY MOBILE WIRELESS E-MAIL SERVICE (GOVERNMENT-PROVIDED HANDHELD DEVICE, NMCI-PROVIDED WIRELESS SERVICE) ($131 MONTHLY) IS THE SAME AS FULL BLACKBERRY SERVICE BUT WITH A GOVERNMENT-PROVIDED BLACKBERRY HANDHELD DEVICE THAT MEETS THE MINIMUM SPECIFICATIONS LISTED IN THE BLACKBERRY SERVICE CLIN (RIM MODELS 857/957 ONLY). RIM MODELS 850/950 ARE NOT SUPPORTED. EDS IS ONLY RESPONSIBLE FOR SLA PERFORMANCE INSIDE THE NMCI INFRASTRUCTURE POINT OF PRESENCE (POP). EDS WILL PROVIDE HELP DESK SUPPORT FOR THE ACCESSED SERVICES PROVIDED FROM EDS AND THE NMCI INFRASTRUCTURE EXCEPT FOR THE GOVERNMENT-PROVIDED AND MAINTAINED HANDHELD DEVICE. IF EDS DETERMINES THAT THE CAUSE OF A REPORTED PROBLEM IS THE RESULT OF THE GOVERNMENT-PROVIDED HANDHELD DEVICE OR NON-CERTIFIED SOFTWARE FAILURE, THE HELP DESK WILL CLOSE THE TROUBLE TICKET AND REFER THE USER TO THEIR GOVERNMENT REPRESENTATIVE FOR RESOLUTION. COSTS ASSOCIATED WITH CHANGES (DEACTIVATION OR REACTIVATION) TO THE CURRENT USERS WIRELESS SUPPORT/PROVIDERS ARE NOT INCLUDED IN THIS CLIN AND ARE THE RESPONSIBILITY OF THE GOVERNMENT.
C. HYBRID BLACKBERRY MOBILE WIRELESS E-MAIL SERVICE (GOVERNMENT-PROVIDED HANDHELD DEVICE AND WIRELESS SERVICE) ($79 MONTHLY) IS THE SAME AS FULL BLACKBERRY SERVICE CLIN BUT WITH A GOVERNMENT-PROVIDED BLACKBERRY HANDHELD DEVICE THAT MEETS THE MINIMUM SPECIFICATIONS LISTED IN THE BLACKBERRY SERVICE CLIN (RIM MODELS 857/957 ONLY). RIM MODELS 850/950 ARE NOT SUPPORTED. GOVERNMENT-PROVIDED COMMERCIAL WIRELESS SERVICE IS NECESSARY FOR INTERFACE WITH THE NMCI-PROVIDED SERVICES AND INFRASTRUCTURE. EDS IS ONLY RESPONSIBLE FOR SLA PERFORMANCE INSIDE THE NMCI INFRASTRUCTURE POINT OF PRESENCE (POP). EDS SHALL PROVIDE HELP DESK SUPPORT FOR THE ACCESSED SERVICES PROVIDED FROM EDS AND THE NMCI INFRASTRUCTURE EXCEPT FOR THE GOVERNMENT-PROVIDED AND MAINTAINED HANDHELD DEVICE AND/OR GOVERNMENT-PROVIDED WIRELESS SERVICE. IF EDS DETERMINES THAT THE CAUSE OF A REPORTED PROBLEM IS THE RESULT OF THE GOVERNMENT-PROVIDED HANDHELD DEVICE, THE GOVERNMENT-PROVIDED WIRELESS SERVICE OR NON-CERTIFIED SOFTWARE FAILURE, THE HELP DESK WILL CLOSE THE TROUBLE TICKET AND REFER THE USER TO THEIR GOVERNMENT REPRESENTATIVE FOR RESOLUTION.

10. SHARED STORAGE. NMCI PROVIDES 800MB OF SHARED STORAGE SPACE FOR EACH NMCI ACCOUNT. IF ADDITIONAL STORAGE IS REQUIRED, ADDITIONAL FILE SHARE SERVICES CAN BE PURCHASED, IN BLOCKS OF 10GB ($31.27 PER MONTH PER BLOCK). THIS SERVICE IS NOT AVAILABLE FOR HYBRID SEATS OR WALL PLUG SERVICES. WE ARE ALSO WORKING TO DEVISE A PROCESS THAT WILL ALLOW US TO MANAGE STORAGE AND MOVE-ADD-CHANGES AT AN ENTERPRISE LEVEL TO PREVENT UNNECESSARY EXPENDITURES AT THE LOCAL COMMAND LEVEL.

11. CLASSIFIED NMCI SEATS. WE UNDERSTAND THE IMPORTANCE OF ASSURED CONNECTIVITY FOR CLASSIFIED NETWORKS IN MEETING CRITICAL C2 REQUIREMENTS. WE ARE REVIEWING THE ABILITY OF THE SECURE ARCHITECTURE PROPOSED BY EDS TO MEET MARINE CORPS NEEDS WHILE REMAINING COMPLIANT WITH DOD REGULATIONS. WE ARE ALSO EVALUATING PROJECTED COSTS OF BOTH NMCI AND NON-NMCI ALTERNATIVES FOR CLASSIFIED SEATS.

12. MARINE CORPS AVIATION INTEROPERABILITY WITH NMCI. REF B IS A MARFORPAC, MARFORLANT AND MARFORRES COORDINATED MESSAGE THAT PROPOSES MARINE AVIATION LOGISTICS SQUADRON (MALS), WITHIN A NAVAL TACTICAL COMMAND SUPPORT SYSTEM (NTCSS) NETWORK DOMAIN, HOSTS MARINE AIR GROUP (MAG) NETWORK GARRISON REQUIREMENTS. IN GARRISON, THE NTCSS NETWORK WOULD BE CONNECTED TO NMCI AS AN EXTERNAL NETWORK. THIS PROPOSAL USES EXISTING NMCI CONTRACT LINE ITEMS TO SUPPORT MARINE AVIATION UNITS IN A WAY SIMILAR TO NAVY'S INTEGRATED SHIPBOARD NETWORK SYSTEM (ISNS) PIERSIDE CONNECTIVITY. AS THIS IS A PROPOSED CHANGE IN CURRENT MARINE CORPS NMCI SEAT ORDERS, HQMC C4, HQMC AVN ASL AND PM-NMCI ARE PRESENTLY REVIEWING THE CONTRACTUAL AND FINANCIAL RAMIFICATIONS OF THIS PROPOSAL. UNITS ARE TO CONTINUE TO COMPLETE SEAT ORDERS AND PRE-AOR PREPARATIONS UNTIL FURTHER NOTICE.

13. NMCI STAKEHOLDERS' COUNCIL (SHC). THE BI-WEEKLY SHC VIDEO TELECONFERENCE, CO-CHAIRED BY HQMC C4, PROVIDES AN OPPORTUNITY FOR MAJOR COMMANDS TO PROJECT FORWARD AND INFLUENCE FUTURE PLANS, VICE REMAINING LOCKED IN THE REACTION MODE. RECOMMEND CONTINUED PARTICIPATION BY MCTOICS IN THIS VALUABLE FORUM.

14. WEB SITES. THE MARINE CORPS NMCI INFORMATION WEB SITE AT HTTPS:(DOUBLE_SLASH)WWW.NMCIINFO.USMC.MIL CONTAINS A LIST OF ANSWERS TO NMCI FREQUENTLY ASKED QUESTIONS (FAQS). IT IS INTENDED TO PROVIDE GUIDANCE TO COMMAND NMCI REPRESENTATIVES/USERS ON COMMONLY ENCOUNTERED ISSUES. THIS SITE IS ACCESSIBLE TO ALL USMC.MIL USERS. ALL NMCI WEBSITES CAN ALSO BE ACCESSED AT THE HQMC C4 WEB SITE HTTP:(DOUBLE_SLASH)HQUSMC.HQMC.USMC.MIL/C4.

15. USMC NMCI CUSTOMER RELATIONS MANAGER. MS. L. LUKSCHANDER (DSN: 278-0213/E-MAIL: LUKSCHANDERLA@MCSC.USMC.MIL) IS AN ADDITIONAL RESOURCE AVAILABLE TO ASSIST CTRS AND OTHER COMMAND REPRESENTATIVES WHO HAVE NMCI ISSUES THAT CANNOT BE RESOLVED AT THE LOCAL LEVEL. ALSO, ALL MEDIA INTERVIEWS, PRESS RELEASES, ETC. MUST BE COORDINATED THROUGH MS. LUKSCHANDER, WHO IN TURN WILL GET APPROVAL FROM DIR NMCI OFFICE AND HQMC PAO PRIOR TO THE INTERVIEW OR PRESS RELEASE.//

BT
#3399
NNNN

D12. 021700Z MAY 03

Subject: INTERIM APPROVAL TO OPERATE (IATO) THE UNCLASSIFIED NMCI TRANSITIONAL BOUNDRY TWO POLICY
Importance: Low

SUBJ/INTERIM APPROVAL TO OPERATE (IATO) THE UNCLASSIFIED
/NMCI TRANSITIONAL BOUNDARY TWO POLICY//

REF/A/DOC/SPAWAR PMW 161/04MAR2003/4A2-086/-/NOTAL//
REF/B/DOC/SPAWAR PMW 164/04MAR2003/4A2-085/-/NOTAL//
REF/C/DOC/NETWARCOM/04MAR2003//
NARR/REF A IS SPAWAR PMW 161 LTR OF RECOMMENDATION FOR B2 IMPLEMENTATION; REF B IS SPAWAR PMW 164 ENDORSEMENT OF THE TRANSITIONAL B2 POLICY; REF C TRAFFIC POLICY MONITOR DEVICE CAPABILITY REQUIREMENTS//
POC/BOB TURNER/CIV/NETWARCOM/LOC:NAB LCRK/TEL:(757) 417-6776 EXT 2
/EMAIL:ROBERT.TURNER@NETWARCOM.NAVY.MIL//
POC/JOHN ROSS/LCDR/NETWARCOM/LOC:NORFOLK,VA/TEL:(757) 417-6776 EXT 1
/EMAIL:JOHN.ROSS(AT)NETWARCOM.NAVY.MIL//

RMKS/1. THROUGH THE NMCI EFFORT, THE NAVY HAS EMBARKED ON AN AGGRESSIVE PROJECT FOR THE SEEMLESS NETWORKS INSIDE THE INTRANET AND A TRANSITIONAL DEFENSE-IN-DETH POSTURE DURING THE CUTOVER PROCESS FROM LEGACY NETWORKS. IN SUPPORT OF THIS EFFORT, THE TRANSITIONAL BOUNDARY TWO FIREWALL POLICY WAS DEVELOPED. BOUNDARY TWO FIREWALL POLICY WAS DEVELOPED.

2. THE NMCI OPERATIONAL DESIGNATED APPROVING AUTHORITY (DAA) GRANTS AN INTERIM APPROVAL TO OPERATE (IATO) FOR A PERIOD NTE ONE (1) YEAR ON THE UNCLASSIFIED NMCI NETWORK USING THE BELOW ENTERPRISE-WIDE B2 POLICY. THIS B2 POLICY SUPERSEDES ALL OTHER B2 POLICIES PREVIOUSLY RELEASED. ALLOWED PORTS AND PROTOCOLS (B2 POLICY LISTED WITHOUT RESTRICTIONS OR COMMENTS) OUTBOUND (FROM THE NMCI ENCLAVE) PORT SERVICE UDP TCP ALL ALL ALL ALL
INBOUND (TO THE NMCI ENCLAVE FROM AOR'D LEGACY NETWORK) PORT SERVICE
UDP TCP 25 SMTP X
80 HTTP X 102 X.400 X
137-138 NETBIOS X X
135,139 NETBIOS X
443 HTTPS X
1433 SQL X

3. THE NMCI TRANSITIONAL BOUNDARY TWO POLICY IS APPROVED WITH THE FOLLOWING CAVEATS:
A. ONLY THOSE LEGACY APPLICATIONS/DEVICES/SERVERS THAT HAVE BEEN REVIEWED BY THE NMCI CONNECTION APPROVAL REVIEW PANEL (NCARP) AND/OR APPROVED BY THE OPERATIONAL DAA ARE PERMITTED TO COMMUNICATE THROUGH B2.

B. ISF WILL CONTINUE TO PROVIDE A WEEKLY FORMAL WRITTEN STATUS REPORT UPDATING THE RESOLUTION OF ISSUES IDENTIFIED IN THE IATO TASK UNCLAS SUBJ: INTERIM APPROVAL TO OPERATE (IATO) THE UNCLASSIFIED NMCI TRANSI LIST. REPORTS ARE TO BE PROVIDED TO PMW 161, CNO (N6143), AND NETWARCOM (N64).

C. ALL TROUBLE REPORTS AND RECOMMENDATIONS FOR CORRECTING VULNERABILITIES IDENTIFIED IN THE SECURITY TESTING AND EVALUATION (ST&E) AND REFERENCE (A) ARE TO BE ADDED TO THE IATO TASK LIST AND TRACKED UNTIL COMPLETION. ALL HIGH

VULNERABILITIES MUST BE MITIGATED TO MEDIUM OR BELOW PRIOR TO CONNECTION TO NMCI.

D. AFTER COMPLETION OF OPERATIONAL TESTING, THIS IATO WILL BE REVISITED WITH ADDITIONAL REQUIREMENTS ADDED, IF NECESSARY.

E. PREMISE ROUTER INTERFACE BETWEEN LEGACY NETWORK AND LEGACY SERVICE PROVIDER CONFIGURED TO ALLOW ONLY THAT TRAFFIC REQUIRED FOR LEGACY SERVICES.

F. THE LEGACY NETWORK PREMISE (OR SEC RTR) CONNECTING TO EXTERNAL NETWORKS (I.E., NIPR, SMARTLINK, DREN) MUST IMPLEMENT AN ACL TO PREVENT TRAFFIC FROM ROUTING THROUGH THE LOCAL LEGACY TO B2 CONNECTION AND SUBSEQUENTLY NMCI. THIS CONFIGURATION SHOULD ALSO INCLUDE RULES TO PREVENT IP SPOOFING.

4. THE B2 POLICY WILL ALLOW ALL OUTBOUND-INITIATED CONNECTIONS TO THE LEGACY LAN IP SPACE AND WILL BE CONSTRAINED BY ACLS. INBOUND INITIATED CONNECTIONS FROM THE LEGACY LAN SHALL BE LOCKED DOWN TO SPECIFIC SERVER IP AND RESTRICTED TO THE MINIMUM NUMBER OF PORTS REQUIRED FROM THOSE LISTED IN PARA 2 ABOVE.

NETWORK SECURITY DEVICES ARE REQUIRED AT THE B2 INTERFACE AND THE LEGACY NETWORK. NETWORK SECURITY DEVICES ARE ALSO REQUIRED AT THE LEGACY NETWORK INNER ROUTER OF THE POP/FIREWALL, AS APPROPRIATE.
A. ONE OF THE SECURITY DEVICES WILL INCLUDE A TRAFFIC POLICY MONITOR. THE POLICY MONITOR MUST HAVE THE ABILITY TO UNWRAP "TUNNELED" TRAFFIC TO ACCURATELY REPORT PORT USAGE. THE POLICY MONITOR NEEDS TO HAVE THE CAPABILITIES IDENTIFIED IN REFERENCE (C). B. NETWARCOM HAS REVIEWED AND APPROVED SECURIFY TO MEET THIS REQUIREMENT. OTHER PRODUCTS CAN BE USED WITH DAA APPROVAL.

6. DIR NMCI/PMO WILL ENSURE, PRIOR TO IMPLEMENTING THIS POLICY, THE FOLLOWING REPORTS ARE COMPLETED AND SUBMITTED TO THE DAA'S OFFICE FOR FINAL ASSESSMENT: DEPLOY NETWORK MONITORING DEVICES AND REPORT ALL UTN PROTECT POLICY NON-COMPLIANCE, A COMPLETE LIST OF LEGACY SYSTEM COMPONENTS AND ASSOCIATED HOST NAMES AND IP ADDRESSES CORRELATED TO PROGRAM OF RECORD NAMES, SITE SSAA REVIEW FOR ACCURACY, VERIFY IAVA COMPLIANCE ON THE LEGACY NETWORK AND A FIWC VULNERABILITY TEST RUN AS AN EXTERNAL PLAYER TO THE LEGACY NETWORK. THE INFORMATION ASSURANCE MANAGER (FORMERLY THE LOCAL DAA) IS REQUIRED TO CORRECT ALL DISCREPANCIES WITHIN THE SPECIFIED TIME FRAME DESIGNATED BY THE NMCI DAA.

7. IMPLEMENTATION OF THE B2 POLICY WILL START AT AOR AND CONTINUE WHILE LEGACY NETOWRK REQUIREMENT REMAINS. WITH THE EXCEPTION OF NMCI/IT21 B2 INTERFACE, ISF IS REQUIRED TO MODIFY ALL EXISTING LEGACY B2'S TO THIS BASELINE AS SOON AS POSSIBLE (REPORT WHEN ALL MOD'S COMPLETE).

8. IN CONJUNCTION WITH AOR PLANS, PMW-161 IATT WILL ASSESS ALL B2 SYSTEMS REGARDLESS OF ITS PLACEMENT IN THE CYCLE.

9. A CONCERTED APPROACH BY THE DIR NMCI, ISF AND NAVY COMMANDS WILL WORK TO REMOVE ALL B2S FROM THE NMCI ARCHITECTURE BY 30 JUNE 2004. QQQQ

10. THIS CERTIFICATION APPROVAL IS GRANTED CONTINGENT ON THE CONTINUED ASSESSMENT BY THE NAVY CERTIFICATION AUTHORITY (PMW-161) THAT CONTINUED ACCEPTABLE PROGRESS IS BEING MADE.

11. ANY QUESTIONS OR COMMENTS CAN BE REFERRED TO THE POCS ABOVE.

12. THIS POLICY CANCELS ALL PREVIOUS NMCI BASELINE B2 POLICIES.//

BT
#0039
NNNN

D13. 052237Z MAY 03 COMLANTFLT NORFOLK VA

Subject: NMCI LEGACY APPLICATIONS PROCESS

Subject: NMCI LEGACY APPLICATIONS PROCESS//
P 052237Z MAY 03 COMLANTFLT NORFOLK VA
TO ALLANTFLT
INFO CNO WASHINGTON DC
ATTENTION INVITED TO ADMINISTRATIVE MESSAGE
PRIORITY
UNCLAS //N03420//
MSGID/GENADMIN/COMLANTFLT//
SUBJ/NMCI LEGACY APPLICATIONS PROCESS//
REF/A/GENADMIN/CNO/252250ZFEB2002//
REF/B/GENADMIN/CNO/301245ZSEP2002//
NARR/REFS A AND B ARE CNO REQUEST FOR ALL COMMANDS TO GET ISF TOOLS IN DADMS//
POC/KOONCE/YNCS/CLF N1S5/-/TEL:DSN:836-4186/TEL:COM:757-836-4186//
RMKS/1. THIS IS AN UNNUMBERED ALLANTFLT MESSAGE.

2. THE MID-TERM FUNCTIONAL AREA MANAGER (FAM) APPLICATION RATIONALIZATION PROCESS MUST BE COMPLETED BY 23 MAY. APPLICATIONS THAT WERE APPROVED DURING THE SHORT-TERM PROCESS (COMPLETED 31 DECEMBER 2002) ARE THE INPUT FOR THE MID-TERM PROCESS. AT THE END OF THE MID-TERM, EACH FAM WILL PRODUCE THREE LISTS INDICATING (1) PREFERRED NAVY APPLICATIONS, (2) NAVY APPLICATIONS ALLOWED WITH RESTRICTION, AND (3) DISAPPROVED. 7,000 APPLICATIONS ACROSS ALL FAMS WERE APPROVED COMING OUT OF SHORT-TERM. BY 23 MAY, THE LIST OF PREFERRED NAVY APPLICATIONS MUST BE NO MORE THAN 3,200 (AS CURRENTLY PROJECTED). NOTE: QUESTIONNAIRES MUST BE COMPLETED BY COB, FRIDAY, 11 MAY
2003. EXPLANATION OF LISTS:
(1) PREFERRED NAVY APPLICATIONS - APPROVED FAM PORTFOLIO FOR NMCI AND NON-NMCI USE.
(2) NAVY APPLICATIONS ALLOWED WITH RESTRICTION - USERS MUST BEGIN USING PREFERRED NAVY APPLICATIONS WITHIN A TIME PERIOD SPECIFIED BY THE FAM. THESE APPLICATIONS MAY BE USED ON NMCI SEATS UNTIL MIGRATION TO PREFERRED NAVY APPLICATIONS BECOMES MANDATORY.
(3) DISAPPROVED - APPLICATIONS THAT DO NOT MAKE IT THROUGH THE MID-TERM PROCESS WILL NOT BE ALLOWED ON NAVY COMPUTERS AND WILL BE REMOVED FROM NMCI SEATS.

3. CMD FAM REPS SHOULD ACCESS THE DADMS WEBSITE AT HTTPS:/WWW.DADMS.NAVY.MIL. FOR NEW USERS, ON THE OPENING SCREEN SELECT ACCESS REQUEST ON THE LEFT HAND SIDE. FOR LOGIN ID, YOU CAN USE YOUR CURRENT EMAIL ADDRESS. SPONSOR INFORMATION IS AS FOLLOWS:
SPONSOR NAME: DOUGLAS BURNS
SPONSOR ORGANIZATION-ORG CODE: SPAWAR-ITC40D
SPONSOR EMAIL: DOUGLAS.BURNS@NAVY.MIL
SPONSOR PHONE: 504-697-2305
REASON FOR ACCESS: QUESTIONNAIRE ACCESS.
FOR CURRENT USERS AND AFTER NEW USERS HAVE OBTAINED DADMS ACCESS, NICK YOUNG OR DOUGLAS BURNS WILL ISSUE YOU ADMIN QST AND APM PRIVILEGES. THIS WILL ALLOW YOU TO FILL IN ADMIN QUESTIONNAIRES ONLY.
QUESTIONNAIRE PROCESS:
(1) LOGIN.

(2) SELECT FAM OPTIONS (LEFT HAND SIDE OF SCREEN).
(3) SELECT FAM MAIN (LEFT HAND SIDE OF SCREEN).
(4) SELECT ADMINISTRATION (DROP DOWN BOX TOP CENTER OF SCREEN).
(5) CLICK "TOTAL ACTIVE - TOTAL" ON MID-TERM RATIONALIZATION APPLICATIONS SUMMARY. NOTE: YOUR SPECIFIC APPLICATION MAY BE IN TOTAL ACTIVE, QUESTIONNAIRE REQUIRED, INS INFO, OR RECLAMAS. MODIFY THIS STEP AS REQUIRED.

4. IN APPLICATION ID, ENSURE ISF IS SELECTED, AND IN THE NEXT BOX ENTER YOUR APP ISF # (PROVIDED). NOTE: YOU CAN ALSO SCROLL/PAGE DOWN UNTIL YOU FIND YOUR APPLICATION.

5. IF YOU CLICK ON THE APPLICATION NAME, A DROP DOWN LIST APPEARS. SELECTING APP QUESTIONNAIRE AT THIS POINT TAKES YOU TO STEP 1 OF A SIX STEP PROCESS:
STEP 1: APPLICATION EDIT SCREEN (FILLED IN BY FAM, CDA, OR STEWARD)
STEP 2: UIC STAKEHOLDER ASSOCIATION AND QUESTIONNAIRE (FILLED IN BY EACH UIC) WAIVER QUESTIONNAIRE FOR RECLAMAS
STEP 3: ASSOCIATED APPLICATION POC
STEP 4: EDIT PARENT APP
STEP 5: ASSOCIATED APP DATABASE INFORMATION
STEP 6: QUESTIONNAIRE (FILLED IN BY CDA OR STEWARD)
(NOTE: EACH STEP MUST BE INDIVIDUALLY SUBMITTED AND CAN BE MODIFIED AFTER SUBMIT.)

6. NOTIFY ADMIN FAM SUPPORT TEAM (OR YOUR CHAIN OF COMMAND) WHEN QUESTIONNAIRE PROCESS IS COMPLETE.
ADDITIONAL INFORMATION:
THE ADMIN FAM SUPPORT TEAM FOR
GOTS/COTS: DOUGLAS.BURNS@NAVY.MIL, 504-697-2305;
RECLAMAS: NICHOLAS.YOUNG@NAVY.MIL, 504-697-2523;
COMLANTFLT POC: ANTHONY.KOONCE@NAVY.MIL, 757-836-4186
WILL ASSIST YOU WITH ANY ISSUES YOU MAY HAVE.
DOUGLAS J. BURNS
SPECIAL PROJECTS MANAGER
SOFTWARE ENGINEERING AND SUSTAINMENT (ITC40)
SPAWAR INFORMATION TECHNOLOGY CENTER
2251 LAKESHORE DRIVE
NEW ORLEANS, LA 70145
SPAWAR (NOLA): 504-697-2305
CELL: 228-623-2904
BUSINESS EMAIL: DOUGLAS.BURNS@NAVY.MIL
PERSONAL EMAIL: IRISHBURNS@HOTMAIL.COM
TEMPORARY ASSIGNMENT:
ADMINISTRATION FAM SUPPORT TEAM LEAD
PEO-IT (WASHINGTON DC)//

BT
#2573
NNNN

D14. 151858Z JUL 02

Subject: NMCI ORDERING INTERFACE SYSTEM (NOIS)

151858Z JUL 02
Subject: NMCI ORDERING INTERFACE SYSTEM (NOIS)//
UNCLAS
MSGID/GENADMIN/PEO-IT WASHINGTON DC/0014//
SUBJ/NMCI ORDERING INTERFACE SYSTEM (NOIS)//
RMKS/1. REQUEST ECHELON 2 CLAIMANTS DISSEMINATE AS APPROPRIATE.
2. THIS MESSAGE ANNOUNCES THE INITIAL OPERATIONAL DEPLOYMENT OF THE NMCI ORDERING INTERFACE SYSTEM (NOIS) ON 22 JULY 2002. THE USE OF NOIS WILL BE MANDATORY FOR PLACING NEW NMCI ORDERS FOR FY03 AND BEYOND. COMMANDS WITH EXISTING ACTIVE SEAT ORDERS MUST TRANSITION TO NOIS BEFORE FY03.
3. BACKGROUND: IN RESPONSE TO MULTIPLE REQUESTS FROM NAVY CLAIMANTS AND USMC, AND AT THE DIRECTION OF ASN (RDA), THE DIRECTOR OF NMCI CHARTERED A TEAM TO DEVELOP AN INTEGRATED ORDER TO DELIVERY (IOD) PROCESS THAT WOULD CONSOLIDATE THE NUMEROUS SYSTEMS AND PROCESSES USED TO FULFILL DON SEAT REQUIREMENTS ON THE NMCI CONTRACT. THIS TEAM LOOKED AT THE ENTIRE PROCESS FROM PLANNING, THROUGH REQUIREMENTS DETERMINATION, PLACING SEAT ORDERS, MONITORING DELIVERY, AND INVOICE RECONCILIATION ON THE BACK END OF THE PROCESS. THE IOD TEAM FOCUSED ON REDUCING DUPLICATE DATA ENTRY THROUGHOUT THE PROCESS. CRITICAL SYSTEMS INVOLVED WITH THE IOD PROCESS INCLUDE: THE NMCI ORDERING INTERFACE SYSTEM (NOIS), THE NMCI EMARKETPLACE, ISF TOOLS, CLAIMANT/DON FINANCIAL MANAGEMENT SYSTEMS, THE SPAWAR FINANCIAL MANAGEMENT SYSTEM, THE ISF ASSET MANAGEMENT SYSTEM, THE ISF STAGING DATABASE, THE ISF BILLING SYSTEM, AND STARS ONE PAY. THE IOD PROCESS AND SYSTEM INTERACTIONS HAVE BEEN DEPICTED GRAPHICALLY AND ARE AVAILABLE ON THE PEO-IT WEB SITE AT HTTP:/WWW.PEO-IT.NAVY.MIL/MEDIA/NMCI%20IOD%20END%20TO%20END.GIF QUESTIONS REGARDING THESE DIAGRAMS SHOULD BE ADDRESSED TO MS. JILL COOKE (COOKEJ@SPAWAR.NAVY.MIL OR PHONE 703-795-2605). THE NMCI EXECUTION PLAN WILL BE UPDATED TO REFLECT THE IOD PROCESS.
4. NMCI ORDERING INTERFACE SYSTEM (NOIS): THE NMCI ORDERING INTERFACE SYSTEM HAS BEEN DESIGNED TO SERVE AS THE CUSTOMER INTERFACE TO THE IOD PROCESS. IT WAS DEVELOPED BY THE NOIS WORKING GROUP, MADE UP OF REPRESENTATIVES FROM NAVY CLAIMANTS AND THE USMC. KEY CONTRIBUTORS INCLUDE: AAUSN, CNET, CPF, MSC, NAVAIR, NAVSEA, AND USMC. NOIS WAS SELECTED AFTER SEVERAL PRODUCT DEMONSTRATIONS OF EXISTING TOOLS. NOIS IS BEING RELEASED USING A PHASED APPROACH. THE FIRST PHASE OF NOIS SUPPORTS USER PROFILES, USER TO APPLICATION/PERIPHERAL MAPPING, AND AN AUTOMATED INTERFACE TO THE EMARKETPLACE. INITIAL RELEASE IS SCHEDULED FOR 22 JULY. INFORMATION ON THE SPECIFIC FUNCTIONALITY OF NOIS AND ITS SUBSEQUENT RELEASE SCHEDULE IS POSTED ON THE PEO-IT WEB SITE AT HTTP:/WWW.PEO-IT.NAVY.MIL/MEDIA/NOIS%20BACKGROUND%20DOCUMENT.DOC
5. FOR FY03, NOIS WILL BE THE ONLY METHOD FOR NAVY CLAIMANTS AND USMC TO ENTER NMCI ORDERS. CLAIMANTS WHO PLACE NEW FY02 ORDERS ARE STRONGLY ENCOURAGED TO START USING NOIS IMMEDIATELY. EXISTING FY02 SEAT ORDERS ALREADY IN PROGRESS CAN BE MANAGED VIA CURRENT PROCEDURES. NAVY CLAIMANTS AND THE USMC WILL BE AFFORDED THE OPPORTUNITY TO DO A ONE TIME PER UIC DATA TRANSFER FROM ANY MANAGEMENT INFORMATION SYSTEM CURRENTLY IN USE TO MANAGE NMCI SEAT REQUESTS; UPON COMPLETION OF THE TRANSFER, NOIS WILL BE THE AUTHORITATIVE SOURCE FOR ALL ORDERING DATA.

6. A LIST OF NOIS POCS AT NAVY CLAIMANTS AND THE USMC IS AVAILABLE
ON THE PEO-IT WEBSITE AT
HTTP:/WWW.PEO-IT.NAVY.MIL/MEDIA/DON%20NOIS%20CONTACT%20LIST.XLS.
ANY QUESTIONS REGARDING THE NOIS SYSTEM AND TRAINING SHOULD BE
DIRECTED THROUGH THE MAJOR CLAIMANT/USMC POINTS OF CONTACT. POC FOR
THE OVERALL EFFORT IS MS. JEAN SANLUIS (EMAIL:
SANLUISJR@NAVSEA.NAVY.MIL, PHONE (202) 781-3043).
7. TRAINING IS MANDATORY FOR ALL NAVY CLAIMANTS AND THE USMC PRIOR
TO USE OF THE SYSTEM. TRAINING WILL COVER BASIC USE OF THE
APPLICATION AND DATA IMPORT METHODS AND RULES. A LIST OF CURRENTLY
SCHEDULED NOIS TRAINING SESSIONS IS AVAILABLE ON THE PEO-IT WEB SITE
AT HTTP:/WWW.PEO-IT.NAVY.MIL/MEDIA/NOIS%20TRAINING%20CALENDAR.DOC
TRAINING CAN BE COORDINATED THROUGH MS. DONNA SMITH (EMAIL:
SMITHDM2@NAVAIR.NAVY.MIL, PHONE (301) 342-9853).//
BT
#0001
NNNN

D15. R 231554Z JUL 03

```
ou:COMNAVNETWARCOM NORFOLK VA(uc)

TO  SECNAV WASHINGTON DC(uc)
    CNO WASHINGTON DC
    COMLANTFLT NORFOLK VA(uc)
    COMPACFLT PEARL HARBOR HI
    COMNAVAIRSYSCOM PATUXENT RIVER MD(uc)
    COMNAVRESFOR NEW ORLEANS LA(uc)
    NETC PENSACOLA FL(uc)
    COMSC WASHINGTON DC(uc)
    BUMED WASHINGTON DC(uc)
    COMNAVSUPSYSCOM MECHANICSBURG PA(uc)
    COMNAVSEASYSCOM WASHINGTON DC(uc)
    COMSPAWARSYSCOM SAN DIEGO CA(uc)
    COMNAVPERSCOM MILLINGTON TN(uc)
    COMNAVSECGRU FT GEORGE G MEADE MD
    COMNAVFACENGCOM WASHINGTON DC(uc)
    ONI WASHINGTON DC
    COMNAVSPECWARCOM CORONADO CA(uc)
    DIRSSP WASHINGTON DC(uc)
    COMNAVMETOCCOM STENNIS SPACE CENTER MS(uc)
    CNR ARLINGTON VA(uc)
    DON CIO WASHINGTON DC(uc)
CC  CG MARCORSYSCOM QUANTICO VA
    ASSTSECNAV RDA WASHINGTON DC(uc)
    ASSTSECNAV FM WASHINGTON DC(uc)
    COMNAVNETWARCOM NORFOLK VA(uc)
    USCINCPAC HONOLULU HI
    PEO IT WASHINGTON DC(uc)
    COMNAVSUPSYSCOM DET NORFOLK VA(uc)
    COMNAVSAFECEN NORFOLK VA(uc)
    COMNAVLEGSVCCOM WASHINGTON DC(uc)
    COMNAVNETSPAOPSCOM DAHLGREN VA(uc)
    COMNAVAIRPAC SAN DIEGO CA
    COMNAVAIRWARCENWPNDIV CHINA LAKE CA(uc)
    COMNAVAIRLANT NORFOLK VA
    COMNAVSURFPAC SAN DIEGO CA
    COMNAVSURFLANT NORFOLK VA
    COMNAVREG SW SAN DIEGO CA
    COMMARFORRES(uc)
    COMMARFORPAC(uc)
    COMMARFORLANT(uc)
    COMOPTEVFOR NORFOLK VA(uc)
    CMC WASHINGTON DC(uc)
    DFAS CLEVELAND OH(uc)
    DFAS HQ ARLINGTON VA
    DFAS INDIANAPOLIS IN(uc)
    FISC NORFOLK VA(uc)
    FISC SAN DIEGO CA(uc)
    MSCLNOPAC PEARL HARBOR HI
    NAVPGSCOL MONTEREY CA
    NAVOBSY WASHINGTON DC(uc)
    NAVSUPINFOSYSACT MECHANICSBURG PA(uc)
    NAVSURFWARCEN DET EARLE NJ
    NAVSTKAIRWARCEN FALLON NV
```

NAVSEALOGCEN MECHANICSBURG PA(uc)
NAVFACENGCOM DET NFI PORT HUENEME CA(uc)
NAVSURFWARCENDIV DAHLGREN VA(uc)
NCTSI SAN DIEGO CA(uc)
NAVICP MECHANICSBURG PA(uc)
NCTF-CND WASHINGTON DC(uc)
NAVICP PHILADELPHIA PA(uc)
SPAWARSYSCEN CHARLESTON DET NORFOLK VA
SPAWARSYSCEN SAN DIEGO CA(uc)
SPAWARSYSCEN CHARLESTON SC(uc)
SPAWARSYSCEN NORFOLK DET SAN DIEGO CA(uc)
SPAWARINFOTECHCEN NEW ORLEANS LA(uc)
MITNOC QUANTICO VA

UNCLAS
PASS TO OFFICE CODE:
INFO PEO IT WASHINGTON DC//DIRNMCI//
MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA//
SUBJ/JOINT NETWARCOM-COMSPAWARSYSCOM (PMW-164) TRANSITIONAL B2
/IMPLEMENTATION AND QUICK LOOK ASSESSMENT SCHEDULE//
REF/A/MSG/COMNAVNETWARCOM NORFOLK VA/021700ZMAY2003//
REF/B/MSG/COMNAVNETWARCOM NORFOLK VA/021936ZMAY2003//
REF/C/MSG/COMNAVNETWARCOM NORFOLK VA/162010ZJUN2003//
REF/D/MSG/COMNAVNETWARCOM NORFOLK VA/091600ZJUL2003//
NARR/REF A IS INTERIM APPROVAL TO OPERATE THE UNCLASSIFIED NMCI
TRANSITIONAL BOUNDARY TWO POLICY MESSAGE; REF B IS NIA 04-03 PRE-AOR
INFORMATION ASSURANCE REQUIREMENTS FOR SITE, DAA, PMO AND EDS
MESSAGE; REF C IS THE MODIFIED IMPLEMENTATION GUIDANCE FOR THE NMCI
TRANSITIONAL BOUNDARY TWO POLICY MESSAGE; REF D IS QUICK LOOK
ASSESSMENT PRESENTATION VTC ANNOUNCEMENT//
POC/BOB TURNER/CTR/NETWARCOM/LOC:NAB LCRK/TEL:757-417-6776 EXT 2
/EMAIL:ROBERT.TURNER@NETWARCOM.NAVY.MIL//
POC/JOHN ROSS/LCDR/NETWARCOM/LOC:NORFOLK, VA/TEL:757-417-6776 EXT 1
/EMAIL:JOHN.ROSS@NETWARCOM.NAVY.MIL//
POC/JEANNE BURTON/QLA/-/-/TEL:843-218-4466
/EMAIL:BURTONJ@SPAWAR.NAVY.MIL//
RMKS/1. THIS MESSAGE DESCRIBES THE NMCI LEGACY NETWORK QUICKLOOK
ASSESSMENT PROCESS, PROVIDES THE SCHEDULE FOR SITES THAT WILL
RECEIVE THE QUICKLOOK ASSESSMENT DEPLOYMENT, AND PROVIDES BACKGROUND
FOR THE VTC SCHEDULED FOR 24 JULY. THIS IS A JOINT DIRECTOR NMCI-
NETWARCOM MESSAGE.
2. BACKGROUND. IN ORDER TO SUPPORT THE ROLLOUT OF THE TRANSITIONAL
BOUNDARY TWO FIREWALL POLICY AT SELECTED SITES ON THE NMCI NETWORK
(REFS A AND C) AND TO SUPPORT SITES IN COMPLETING DAA REQUIRED
INFORMATION ASSURANCE DOCUMENTATION FOR NMCI AOR LEGACY NETWORKS
(REF B), NETWARCOM IS SPONSORING A QUICK LOOK ASSESSMENT (QLA)
PROCESS. THE QUICK LOOK ASSESSMENT PROCESS WILL USE IATT QUICKLOOK
ASSESSMENT TEAMS TO CONDUCT ON SITE ASSESSMENTS OF LEGACY NETWORKS
THAT ARE IN AOR OR ARE SCHEDULED TO AOR. FOR THE SITES THAT HAVE
NOT COMPLETED AND DELIVERED THE PRE-AOR INFORMATION ASSURANCE
DOCUMENTATION REQUESTED IN REF B, THE QUICKLOOK ASSESSMENT TEAMS
WILL ACT AS NETWARCOM AGENT IN COLLECTION OF OUTSTANDING
DOCUMENTATION.
3. CONOPS AND DATA SECURITY. AN INBRIEF WILL BE CONDUCTED WITH SITE
PERSONNEL AND SITE CONCURRENCE WILL BE OBTAINED PRIOR TO THE QLAT
COMMENCING THE ASSESSMENT. THE DATA COLLECTED UTILIZING THE

SECURIFY SUITE WILL BE PROTECTED IN TRANSIT FROM THE SITES TO THE SECURIFY ENTERPRISE MANAGER LOCATED AT SSC CHARLESTON. ANY OTHER DATA COLLECTED FROM THE SITE WILL ALSO BE PROTECTED VIA THE CM PRO DOCUMENT MANAGEMENT SYSTEM. THE QLAT WILL OPERATE UNDER A CONOPS THAT ESTABLISHES RULES TO ENSURE SITE COORDINATION AND PROTECTION OF THE INFORMATION COLLECTED.
4. AS INDICATED IN REF A, PARA 6 AND REF C, PARA 2 THE PMO IS DIRECTED TO DEPLOY NETWORK SECURITY DEVICES TO COMPLETE ALL OF THE REQUIRED IA REVIEWS AND REPORTS TO INCLUDE TECHNICAL NETWORK ASSESSMENTS. THESE IA REVIEWS AND REPORTS WILL ALLOW THE DAA TO COMPLETE A SECURITY ASSESSMENT WHICH IS REQUIRED TO CONTINUE WITH THE IMPLEMENTATION OF THE TRANSITIONAL B2 BEYOND THE 45 DAY PERIOD. THE PMO HAS ESTABLISHED QUICK LOOK ASSESSMENT TEAMS (QLAT) TO COMPLETE THE IA REVIEWS AND REPORTS REQUIRED BY NETWARCOM AND HAS BEGUN INITIAL QLA PREPARATION. THE QLAT WILL REVIEW ALL INFORMATION COLLECTED WITH THE SITE PRIOR TO SUBMISSION TO NETWARCOM.
5. THE QLAT WILL PERFORM THE FOLLOWING ACTIONS TO DEVELOP THE IA REVIEWS AND REPORTS THAT WILL PROVIDE NETWARCOM WITH A SITUATIONAL AWARENESS OF LEGACY NETWORK SECURITY POSTURE:
A. UNCLASSIFIED TRUSTED NETWORK PROTECTION POLICY (UTNPP) COMPLIANCE.
(1) INSTALL SECURIFY MONITORING POINTS AT ALL OF THE SITES' LEGACY TRUSTED-TO-UNTRUSTED CONNECTIONS AND COLLECT DATA FOR A MINIMUM OF FIVE DAYS USING THE UTNPP AS A BASELINE.
(2) REVIEW THE SITES' SECURITY PERIMETER DEVICES CONFIGURATIONS AND PROVIDED RECOMMENDATIONS TO IMPROVE THE SITES' OVERALL SECURITY POSTURE.
B. SERVER LIST AND IAVA COMPLIANCE.
(1) COMPARE THE SITE PROVIDED SERVER LIST AND THE DATA CAPTURED BY SECURIFY TO COMPILE A SERVER LIST INCLUDING IP ADDRESSES, DNS NAME, HOST NAME, AND SERVICE.
(2) USE THE SITE PROVIDED IAVA LIST TO CONDUCT RANDOM SERVER CHECKS TO ENSURE VALIDITY OF THE INFORMATION.
C. IDENTIFY CURRENT VULNERABILITIES. NCTF-CND, AS A MEMBER OF THE QLAT, WILL IDENTIFY AND VALIDATE POTENTIAL NETWORK VULNERABILITIES AND OUTSIDE THREATS BY CONDUCTING AN ON-LINE SURVEY (OLS).
D. DETERMINE THE CURRENT CERTIFICATION AND ACCREDITATION POSTURE OF THE LEGACY NETWORK. CONDUCT AN ASSESSMENT OF THE SITES' SSAA(S) AND IATO(S) TO DETERMINE IF ALL OF THE SITES' APPLICATIONS, SERVERS, AND SYSTEMS HAVE BEEN IDENTIFIED.
6. A TECHNICAL ASSESSMENT WILL BE CONDUCTED ON ALL INFORMATION RECEIVED TO ASSIST THE SITE, PMO, AND NETWARCOM IN MITIGATING LEGACY NETWORK RISKS TO IMPROVE THE SECURITY POSTURE OF THE LEGACY NETWORK. THE QLAT WILL PROVIDE AN OUT-BRIEF AT THE END OF THE SCHEDULED DEPLOYMENT PERIOD FOR THE SITE WITH PMO AND NETWARCOM TO PROVIDE QLA RESULTS.
7. THE QLAT WILL OBTAIN AND UTILIZE THE DOCUMENTS PROVIDED BY THE SITE ISSM AND LOCAL IA MANAGERS TO NETWARCOM AS OUTLINED IN REF B, PARA 3. THIS INFORMATION IS INDICATED AS REQUIRED BELOW. IN ADDITION TO THE REQUIRED DOCUMENTATION, THE SITE ISSM AND LOCAL IA MANAGER ARE REQUESTED TO PROVIDE THE SUPPLEMENTAL INFORMATION AS OUTLINED BELOW TO THE REGIONAL QLA LEAD UPON REQUEST IF NOT PREVIOUSLY SUBMITTED. SITE ISSM(S) AND LOCAL IA MANAGER(S) ARE REMINDED TO SUBMIT THEIR DOCUMENTATION AS OUTLINED IN REF A-C TO ROBERT TURNER/TEL:757-417-6776
(ROBERT.TURNER(AT)NETWARCOM.NAVY.MIL).
A. NETWORK INFRASTRUCTURE DOCUMENTATION (REQUIRED)
(1) CURRENT AND ACCURATE NETWORK ARCHITECTURE DIAGRAMS INCLUDING

ROUTER, SWITCHES, FIREWALLS, AND SERVER PLACEMENTS.
(2) SITE CONCURRENCE MEMORANDUM (SCM), PRELIMINARY SITE QUESTIONNAIRE (PSQ), AND RATIONALIZED LIST.
B. VULNERABILITY DOCUMENTATION (REQUIRED)
(1) LETTER OF ASSURANCE THAT THERE ARE NO EXTERNAL OR "BACK DOOR" CONNECTIONS AND/OR LIST THOSE CONNECTIONS AUTHORIZED BY THE OFFICIAL APPROVED EXCEPTION THROUGH OPNAV.
(2) ON-LINE SURVEYS (OLS) WILL BE CONDUCTED DURING THE QLA DEPLOYMENT. AN OLS REQUEST MUST BE SUBMITTED. REQUEST FORMS ARE AVAILABLE VIA THE FOLLOWING URL: HTTP:/WWW.NAVCIRT.NAVY.MIL/OLS.SHTML. SELECT NAVCIRT FORMS AND THEN SELECT ON-LINE SURVEYS. USE THE COMMENT FIELDS TO INDICATE A QLA OLS BASED REQUEST.
C. CERTIFICATION AND ACCREDITATION DOCUMENTATION (REQUIRED)
(1) SSAA
(2) IATO/ATO
(3) NETWORK RISK STATEMENT
(4) LETTER OF ASSURANCE THAT THE NETWORK AND ALL CONNECTIONS ARE OPERATED IN COMPLIANCE WITH THE INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) PROGRAM.
D. SUPPLEMENTAL DOCUMENTATION WILL BE REQUIRED UPON ARRIVAL OF THE QLAT TO ASSIST IN SUCCESSFUL EXECUTION. LOCAL IA MANAGER AND ISSM SHOULD PREPARE FOR THE DELIVERY OF THE FOLLOWING TO THE QLAT:
(1) IP ADDRESS SPACE
(2) DISA NETWORK WAIVERS
(3) SERVER LISTS INCLUDING IP ADDRESSES, SYSTEM IDS, HOST NAMES, AND PURPOSE
(4) LIST OF DOMAIN SERVERS WITHIN THE LEGACY NETWORK.
(5) ACCEPTED COMMUNICATION LIST (PORTS AND PROTOCOLS)
(6) SERVER-TO-APPLICATION MAPPING.
(7) FIREWALL CONFIGURATIONS (INCLUDING: FILTERS, RULES, PROXIES, AND IP ADDRESSES
(8) ROUTER CONFIGURATIONS AND ACLS (PERIMETER ONLY)
(9) LIST OF CURRENT AND PENDING NETWORK CHANGES AND PROJECTS
8. AS SPECIFIED IN REF A, PARA 6 AND REF C, PARA 3 SECURIFY HAS BEEN DESIGNATED AS THE NETWORK SECURITY DEVICE TO COMPLETE THE IA REVIEWS AND A LICENSING AGREEMENT HAS BEEN OBTAINED. THE QLAT WILL ALSO USE THE FOLLOWING ADDITIONAL TOOLS TO ASSIST IN THE COMPLETION OF THE IA REVIEWS AND REPORTS:
NESSUS (NTE 45 DAYS)
KISMET(NTE 45 DAYS)
NMAP(NTE 45 DAYS)
ETHERPEEK(NTE 45 DAYS)
9. NETWARCOM, NMCI DIRECTOR, PMO, NCTF-CND AND EDS/SECURIFY HAVE AGREED TO A QLA SITE DEPLOYMENT SCHEDULE THAT WAS DEVELOPED UTILIZING THE FOLLOWING CRITERIA: SEAT COUNT, OPEVAL, LARGE SITE LOCATION, QUARANTINED SEATS AND DESKTOPS. ADDITIONALLY, EDS TRANSITIONAL B2 PLANS ARE UNDERWAY TO SUPPORT THIS DEPLOYMENT SCHEDULE UPON CERTIFICATION OF THE TRANSITIONAL B2 POLICY AND THE ENTERPRISE CHANGE CONFIGURATION BOARD (ECCB) APPROVAL FOR THIS POLICY. UPON ECCB APPROVAL, EDS WILL BEGIN IMMEDIATE DEPLOYMENT PLANS TO FOLLOW THE QLAT. UPON SUCCESSFUL PUSH OF THE TRANSITIONAL B2 POLICY, THE 45-DAY PERIOD WILL BEGIN TO MEET REQUIREMENTS OUTLINED IN REF C.
10. THE FOLLOWING SITE LOCATIONS HAVE BEEN SELECTED FOR INITIAL QLA DEPLOYMENT AND BROKEN DOWN BY CLAIMANT FOR THE PURPOSES OF THIS MESSAGE. THE QLAT WILL PROVIDE ASSOCIATED UICS AT THE TIME OF

DEPLOYMENT. UIC SPECIFIC SCHEDULES ARE BEING FINALIZED AND WILL BE POSTED ON THE WEBSITE SPECIFIED IN PARAGRAPH 11.
REGION: NORTHEAST
SITE LOCATION: WASHINGTON NAVY YARD:
CLAIMANT AND QLA START DATES:
AAUSN BEGINS 28 JUL 03
NAVFAC BEGINS 4 AUG 03
MSC BEGINS 11 AUG 03
CNO BEGINS 18 AUG 03
SPAWAR BEGINS 25 AUG 03
NAVSUP BEGINS 2 SEPT 03
RESFOR BEGINS 9 SEPT 03
HQMC BEGINS 17 SEPT 03
CLF BEGINS 24 SEPT 03

REGION: SOUTHWEST
SITE LOCATION: NAVAL AIR STATION NORTH ISLAND
CLAIMANT AND QLA START DATES:
CPF BEGINS 28 JUL 03
NAVAIR BEGINS 4 AUG 03
RESFOR BEGINS 11 AUG 03
CLF BEGINS 18 AUG 03
NETC BEGINS 25 AUG 03
NMOC BEGINS 2 SEPT 03
NAVFAC BEGINS 9 SEPT 03
NAVSUP BEGINS 17 SEPT 03
SECGRU BEGINS 24 SEPT 03

REGION: SOUTHEAST
SITE LOCATION: NAVAL STATION NORFOLK
CLAIMANT AND QLA START DATES:
CLF BEGINS 4 AUG 03
NAVFAC BEGINS 11 AUG 03
NETC BEGINS 18 AUG 03
NAVSUP BEGINS 25 AUG 03
SPAWAR BEGINS 2 SEPT 03
MARFORLANT BEGINS 9 SEPT 03
RESFOR BEGINS 17 SEPT 03
CNO BEGINS 24 SEPT 03
AAUSN 1 OCT 03
MSC BEGINS 8 OCT 03
NAVSEA BEGINS 15 OCT 03
SECGRU BEGINS 22 OCT 03
MARSFORRES STARTS 29 OCT 03
NMOC BEGINS 5 NOV 03
NAVAIR BEGINS 12 NOV 03

REGION: NORTHWEST
SITE LOCATION: NAVAL STATION BREMERTON
CLAIMANT AND QLA START DATES:
NAVAL STATION BREMERTON:
NAVSEA BEGINS 4 AUG 03
SITE LOCATION: NSB BANGOR
CLAIMANT AND QLA START DATES:
CPF BEGINS 17 SEPT 03
NETC BEGINS 24 SEPT 03

AAUSN BEGINS 1 OCT 03
RESFOR BEGINS 8 OCT 03
CLF BEGINS 15 OCT 03
SITE LOCATION: NS EVERETT
CLAIMANT AND QLA START DATES:
NS EVERETT BEGINS 24 OCT 03

REGION: HAWAII
SITE LOCATION: PEARL HARBOR NAVAL COMPLEX
CLAIMANT AND QLA START DATES:
CPF BEGINS 11 AUG 03
NAVFAC BEGINS 18 AUG 03
NAVSUP BEGINS 25 AUG 03
NETC BEGINS 2 SEPT 03
NMOC BEGINS 9 SEPT 03
CLF BEGINS 17 SEPT 03
AAUSN BEGINS 24 SEPT 03
NAVSEA BEGINS 1 OCT 03
SECGRU BEGINS 8 OCT 03

11. A VTC IS CURRENTLY SCHEDULED FOR 24 JULY 03 TO ADDRESS QLA RELATED QUESTIONS, REF D REFERS. QLA DOCUMENTS ARE AVAILABLE FOR DOWNLOAD AND REVIEW AT THE FOLLOWING URL: HTTPS:/INFO.NNSOC.NAVY.MIL/NMCI//

D16. 091600Z JUL 03

```
091600Z JUL 03 COMNAVNETWARCOM NORFOLK VA(uc)

TO  SECNAV WASHINGTON DC(uc)
    CNO WASHINGTON DC
    COMLANTFLT NORFOLK VA
    COMPACFLT PEARL HARBOR HI
    COMNAVAIRSYSCOM PATUXENT RIVER MD(uc)
    COMNAVRESFOR NEW ORLEANS LA(uc)
    NETC PENSACOLA FL(uc)
    COMSC WASHINGTON DC(uc)
    BUMED WASHINGTON DC(uc)
    COMNAVSUPSYSCOM MECHANICSBURG PA
    COMNAVSEASYSCOM WASHINGTON DC
    COMSPAWARSYSCOM SAN DIEGO CA(uc)
    COMNAVPERSCOM MILLINGTON TN(uc)
    COMNAVSECGRU FT GEORGE G MEADE MD
    COMNAVFACENGCOM WASHINGTON DC(uc)
    ONI WASHINGTON DC
    COMNAVSPECWARCOM CORONADO CA(uc)
    DIRSSP WASHINGTON DC(uc)
    COMNAVMETOCCOM STENNIS SPACE CENTER MS(uc)
    CNR ARLINGTON VA(uc)
    DON CIO WASHINGTON DC(uc)
CC  CG MARCORSYSCOM QUANTICO VA
    ASSTSECNAV RDA WASHINGTON DC(uc)
    ASSTSECNAV FM WASHINGTON DC(uc)
    COMNAVNETWARCOM NORFOLK VA(uc)
    USCINCPAC HONOLULU HI
    PEO IT WASHINGTON DC(uc)
    COMNAVSUPSYSCOM DET NORFOLK VA(uc)
    COMNAVSAFECEN NORFOLK VA(uc)
    COMNAVLEGSVCCOM WASHINGTON DC(uc)
    COMNAVNETSPAOPSCOM DAHLGREN VA(uc)
    COMNAVAIRPAC SAN DIEGO CA
    COMNAVAIRWARCENWPNDIV CHINA LAKE CA(uc)
    COMNAVAIRLANT NORFOLK VA
    COMNAVSURFPAC SAN DIEGO CA
    COMNAVSURFLANT NORFOLK VA
    NAVNETSPAOPSCOM DET WASHINGTON DC(uc)
    COMNAVREG SW SAN DIEGO CA
    COMMARFORRES(uc)
    COMMARFORPAC(uc)
    COMMARFORLANT(uc)
    COMOPTEVFOR NORFOLK VA(uc)
    CMC WASHINGTON DC(uc)
    DFAS HQ ARLINGTON VA
    DFAS INDIANAPOLIS IN(uc)
    DIRSSP WASHINGTON DC(uc)
    FISC NORFOLK VA(uc)
    FISC SAN DIEGO CA(uc)
    MSCLNOPAC PEARL HARBOR HI
    NAVPGSCOL MONTEREY CA
    NAVOBSY WASHINGTON DC(uc)
    NAVSUPINFOSYSACT MECHANICSBURG PA(uc)
```

NAVSURFWARCEN DET EARLE NJ
NAVSTKAIRWARCEN FALLON NV
NAVSEALOGCEN MECHANICSBURG PA(uc)
NAVFACENGCOM DET NFI PORT HUENEME CA(uc)
NAVSURFWARCENDIV DAHLGREN VA(uc)
NCTSI SAN DIEGO CA(uc)
NAVICP MECHANICSBURG PA(uc)
NCTF-CND WASHINGTON DC(uc)
NAVICP PHILADELPHIA PA(uc)
SPAWARSYSCEN CHARLESTON DET NORFOLK VA
SPAWARSYSCEN SAN DIEGO CA(uc)
SPAWARSYSCEN CHARLESTON SC(uc)
SPAWARSYSCEN NORFOLK DET SAN DIEGO CA(uc)
SPAWARINFOTECHCEN NEW ORLEANS LA(uc)

UNCLAS
MSGID/GENADMIN/COMNAVNETWARCOM NORFOLK VA//
SUBJ/NMCI QUICK LOOK ASSESSMENT PRESENTATION VTC ANNOUNCEMENT//
REF/A/MSG/COMNAVNETWARCOM NORFOLK VA/021700ZMAY2003//
REF/B/MSG/COMNAVNETWARCOM NORFOLK VA/021936ZMAY2003//
REF/C/MSG/COMNAVNETWARCOM NORFOLK VA/162010ZJUN2003//
NARR/REF A IS INTERIM APPROVAL TO OPERATE THE UNCLASSIFIED NMCI TRANSITIONAL BOUNDARY TWO POLICY MESSAGE; REF B IS NIA PRE-AOR INFORMATION ASSURANCE REQUIREMENTS FOR SITE, DAA, PMO AND EDS MESSAGE; REF C IS THE MODIFIED IMPLEMENTATION GUIDANCE FOR THE NMCI TRANSITIONAL BOUNDARY TWO POLICY MESSAGE.//

POC/BOB TURNER/CIV/NETWARCOM/LOC:NAB LCRK/TEL:757-417-6776 EXT 2 /EMAIL:ROBERT.TURNER@NETWARCOM.NAVY.MIL//
POC/JOHN ROSS/LCDR/NETWARCOM/LOC:NORFOLK, VA/TEL:757-417-6776 EXT 1 /EMAIL:JOHN.ROSS@NETWARCOM.NAVY.MIL//
POC/JEANNE BURTON/QLA/-/-/TEL:843-218-4466 /EMAIL:BURTONJ@SPAWAR.NAVY.MIL//

RMKS/1. REFS A-B ANNOUNCED BOUNDARY TWO AND INFORMATION ASSURANCE REQUIREMENTS FOR NMCI TRANSITION. REF C PROVIDED MODIFIED POLICY GUIDANCE. AS PART OF THE NMCI TRANSITIONAL BOUNDARY TWO INITIATIVE, SPAWAR TEAMS WILL VISIT SITES TO CONDUCT QUICK LOOK ASSESSMENT OF LEGACY NETWORKS CONNECTED TO NMCI.

2. A VIDEO TELECONFERENCE (VTC) WILL BE HELD 24 JULY 03 AT 1400-1530 EST TO DISCUSS REF A-C AND INTRODUCE NMCI PMO QUICK LOOK ASSESSMENT (QLA). REQUEST ACTION ADDEE ISSM(S) AND N6 STAFF REPRESENTATIVES RESPONSIBLE FOR NMCI IMPLEMENTATION AND LEGACY NETWORK INFORMATION ASSURANCE (IA) ATTEND. READ AHEAD PRESENTATION AND QLA SCHEDULE WILL BE PROVIDED SEPCOR. IN ORDER TO ENSURE CLAIMANT CONCERNS ARE ADDRESSED DURING THE LIMITED VTC TIME AVAILABLE, REQUEST REVIEW REF A-C AND PRESENTATION AS READ AHEAD AND FORWARD QUESTIONS TO POC LISTED IN THIS MESSAGE.

3. VTC AGENDA
A. OPENING REMARKS PROVIDED BY CNNWC (05 MINUTES)
B. ISSM GUIDANCE PROVIDED BY CNNWC (10 MINUTES)
C. QLA PRESENTATION (45 MINUTES)
D. QUESTIONS AND ANSWER SESSION (30 MINUTES)

4. THE VTC IS BEING HOSTED BY SPAWAR AND ALL PARTICIPANTS ARE REQUESTED TO PROVIDE THE NAME, TELEPHONE NUMBER AND E-MAIL ADDRESS OF THEIR VTC COORDINATOR TO REBECCA.TERPSTRA@EMAINC.COM NLT 14 JUL 03.

5. REQUEST WIDEST DISTRIBUTION TO ENSURE MAXIMUM PARTICIPATION.//

D17. 162010Z JUN 03

162010Z JUN 03 NETWARCOM

To: All Commands

SUBJ: MODIFIED IMPLEMENTATION GUIDANCE FOR THE NMCI TRANSITIONAL BOUN
DARY TWO POLICY

MSGID/GENADMIN/NETWARCOM//

SUBJ/MODIFIED IMPLEMENTATION GUIDANCE FOR THE NMCI TRANSITIONAL
/BOUNDARY TWO POLICY//

REF/A/RMG/NETWARCOM/021700ZMAY2003//
REF/B/DOC/SPAWAR PMW 161/04MAR2003/4A2-086/-/NOTAL//
REF/C/DOC/SPAWAR PMW 164/04MAR2003/4A2-085/-/NOTAL//
REF/D/DOC/NETWARCOM/04MAR2003//

NARR/REF A IS NETWARCOM INTERIM AUTHORITY TO OPERATE THE
UNCLASSIFIED NMCI TRANSITIONAL BOUNDARY TWO POLICY;
REF B IS SPAWAR PMW 161 LTR OF RECOMMENDATION FOR B2 IMPLEMENTATION;
REF C IS SPAWAR PMW 164 ENDORSEMENT OF THE TRANSITIONAL B2 POLICY;
REF D IS TRAFFIC

POLICY MONITOR DEVICE CAPABILITY REQUIREMENTS//

POC/BOB TURNER/CIV/NETWARCOM/LOC:NAB LCRK/TEL:(757) 417-6776 EXT 2
/EMAIL:ROBERT.TURNER@NETWARCOM.NAVY.MIL//
POC/JOHN ROSS/LCDR/NETWARCOM/LOC:NORFOLK,VA/TEL:(757) 417-6776 EXT 1
/EMAIL:JOHN.ROSS(AT)NETWARCOM.NAVY.MIL//

RMKS/1. THIS MESSAGE REVISES THE IMPLEMENTATION GUIDANCE FOR THE
NMCI-TO-SITE LEGACY SYSTEM TRANSITIONAL B2 POLICY AS ORIGINALLY
PROMULGATED REF A. THIS MODIFICATION IS INTENDED TO ALLOW A QUICKER
IMPLEMENTATION OF THE TRANSITIONAL B2 POLICY WHILE STILL ENSURING
ADEQUATE SECURITY OF THE NMCI NETWORK. THIS MODIFICATION DOES NOT
CHANGE THE POLICY ITSELF (ALLOWED PORTS AND PROTOCOLS AND ASSOCIATED
RESTRICTIONS) AS PROMULGATED IN REF A, PARAGRAPHS 2 THROUGH 5. AS
STATED IN REF A, THIS TRANSITIONAL POLICY APPLIES ONLY TO
NMCI-TO-SITE LEGACY SYSTEM BOUNDARIES AND DOES NOT APPLY TO THE
NMCI-TO-IT21 BOUNDARY.

2. IN SUMMARY, THE MODIFIED IMPLEMENTATION GUIDANCE WILL ALLOW
CONCURRENT IMPLEMENTATION OF THE TRANSITIONAL B2 BETWEEN NMCI AND
LEGACY SITES IN CONJUNCTION WITH DEPLOYMENT OF NETWORK SECURITY
DEVICES AND COMPLETION OF THE REQUIRED IA REVIEWS AND REPORTS FOR A
PERIOD NOT TO EXCEED 45 DAYS. PMO IS CREATING QUICKLOOK ASSESSMENT
(QLA) TEAMS THAT WILL USE THE SECURIFY PRODUCT TO ACCOMPLISH THE
NETWORK MONITORING AND TO ASSIST CLAIMANTS IN COMPLETION OF THE
REQUIRED IA REVIEWS AND REPORTS WITHIN THE 45 DAY TIME LIMIT. IN

ORDER TO CONTINUE OPERATION WITH THE TRANSITIONAL B2 BEYOND 45 DAYS, THE REQUIRED IA REVIEWS AND REPORTS MUST BE COMPLETED TO ALLOW THE DAA TO COMPLETE A SECURITY ASSESSMENT. IF REQUIRED REVIEWS AND REPORTS ARE NOT COMPLETED WITHIN THE 45 DAY PERIOD, FURTHER IMPLEMENTATION OF THE TRANSITIONAL B2 WILL BE HALTED. PMO AND DIR NMCI HAVE APPROVED AN INITIAL SCHEDULE FOR THE IMPLEMENTATION OF THE TRANSITIONAL B2 IN CONJUNCTION WITH THE DEPLOYMENT OF THE PMO QUICKLOOK ASSESSMENT TEAMS. PMO WILL PROMULGATE THE TRANSITIONAL B2 IMPLEMENTATION SCHEDULE AND QUICKLOOK ASSESSMENT GUIDE VIA SEPCOR.

3. IMPLEMENTATION OF THE TRANSITIONAL B2 AT LEGACY SITES MUST OCCUR IN CONJUNCTION WITH DEPLOYMENT OF THE LEGACY NETWORK SECURITY DEVICES. NETWARCOM HAS REVIEWED AND APPROVED SECURIFY TO MEET THIS REQUIREMENT. OTHER PRODUCTS CAN BE USED ONLY WITH DAA APPROVAL. SITES POSSESSING THEIR OWN LEGACY NETWORK SECURITY DEVICES CAN IMPLEMENT THE TRANSITIONAL B2 IN CONJUNCTION WITH THE USE OF THOSE DEVICES SUBJECT TO THE SAME RESTRICTIONS SPECIFIED BELOW AND FOLLOWING THE SAME QUICKLOOK ASSESSMENT PROCEDURE THAT THE PMO TEAMS WOULD EMPLOY.

4. ACTION: THE FOLLOWING IMPLEMENTATION INSTRUCTIONS SUPERCEDE THE INSTRUCTIONS IN REF A PARAGRAPHS 6, 7 AND 8.
A. DIR NMCI/PMO WILL ENSURE THE FOLLOWING ACTIONS AND REPORTS ARE COMPLETED AND SUBMITTED TO THE DAA'S OFFICE FOR FINAL ASSESSMENT:
(1) DEPLOY NETWORK MONITORING DEVICES AND CONDUCT QUICKLOOK ASSESSMENT IN ACCORDANCE WITH PMO QLA GUIDELINES
(2) REPORT ALL UTN PROTECT POLICY NON-COMPLIANCE
(3) SUBMIT A COMPLETE LIST OF LEGACY SYSTEM COMPONENTS AND ASSOCIATED HOST NAMES AND IP ADDRESSES CORRELATED TO PROGRAM OF RECORD NAMES
(4) REPORT COMPLETION OF A SITE SSAA REVIEW FOR ACCURACY
(5) VERIFY AND REPORT IAVA COMPLIANCE ON THE LEGACY NETWORK
(6) COMPLETE A VULNERABILITY TEST RUN AS AN EXTERNAL PLAYER TO THE LEGACY NETWORK (ON-LINE SURVEY).
B. THE TRANSITIONAL B2 POLICY OF REF A MAY BE IMPLEMENTED IN CONJUNCTION WITH INITIATING A LEGACY NETWORK ANALYSIS CONDUCTED BY THE PMO QUICK LOOK ASSESSMENT TEAM. THE ACTIONS AND REPORTS REQUIRED BY PARAGRAPH 4.A ABOVE CAN BE SUBMITTED AS PART OF THE QUICKLOOK ASSESSMENT BUT MUST BE COMPLETED WITHIN THE 45 DAY PERIOD.
C. THE INFORMATION ASSURANCE MANAGER (FORMERLY THE LOCAL DAA) IS REQUIRED TO CORRECT ALL DISCREPANCIES IDENTIFIED DURING THIS ASSESSMENT WITHIN THE SPECIFIED TIME FRAME DESIGNATED BY THE NMCI DAA.

5. PROVIDED THAT DIR NMCI/PMO CONCUR AND PROVIDED THAT THE REQUIREMENTS OF PARAGRAPH 4 ABOVE WILL BE MET WITHIN 45 DAYS, SITES THAT HAVE THEIR OWN LEGACY NETWORK SECURITY DEVICES THAT MEET THE REQUIREMENTS OF REF A PARAGRAPH 5 MAY ALSO IMPLEMENT THE TRANSITIONAL B2 POLICY.

6. NETWORK SECURITY COMPLIANCE AND RESPONSIBILITY IS A CRITICAL WARFIGHTING FUNCTION. NETWORKS ARE PERVASIVE AND MUST BE SECURE AND

INTEROPERABLE TO EFFECTIVELY MEET WARFIGHTER NEEDS. FOR THIS REASON PROJECTIONS THAT DISCREPANCIES WILL BE CLEARED WITHIN 45 DAYS MUST BE BASED ON REASONABLE PROJECTIONS OF TECHNICAL AND RESOURCE CONSTRAINTS. AS NETWARCOM ASSUMES DAA OF LEGACY NETWORKS CLEAR REPORTING OF COMPLIANCE IS REQUIRED.//

BT
#1956
NNNN

D18. 021936Z MAY 03

021936Z MAY 03 COMNAVNETWARCOM NORFOLK VA
TO ALNMCI
CG MARCORSYSCOM QUANTICO VA
INFO COMNAVNETWARCOM NORFOLK VA
SUBJ/NIA 04-03, PRE-AOR INFORMATION ASSURANCE REQUIREMENTS FOR SITE, /DAA, PMO AND EDS//
REF/A/GENADMIN/COMNAVNETWARCOM NORFOLK VA/231902ZDEC2002//
REF/B/DOC/COMNAVNETWARCOM NORFOLK VA/YMD:20021028//
NARR/REF A IS NIA AND NIB PROMULGATION MESSAGE. REF B IS NETWARCOMINST 5239.1 LISTING IA RESPONSIBILITIES.//

POC/BOB TURNER/CONT/COMNAVNETWARCOM/LOC:LITTLE CREEK, VA /TEL:757-417-6776/TEL:757-218-5774 /EMAIL:ROBERT.TURNER(AT)NETWARCOM.NAVY.MIL//
POC/SHALALIA WESLEY/LTJG GLOBAL ISSM/NNSOC GNOC DET NORFOLK /LOC:NORFOLK VA/TEL:(757) 963-1050/EMAIL:SHALALIA.WESLEY(AT)NAVY.MIL //
RMKS/1. PURPOSE: THIS NMCI INFORMATION ADVISORY PROMULGATES INTERIM REQUIREMENTS AND ACTIONS TO BE TAKEN BY SITE IA PERSONNEL AND THE DAA, PMO AND EDS IA TEAMS IN ORDER TO SUPPORT SECURITY REQUIREMENTS OF NMCI AND NETWORKS UNDER ASSUMPTION OF RESPONSIBILITY (AOR).
2. DISCUSSION: NETWORK SECURITY COMPLIANCE AND RESPONSIBILITY IS A CRITICAL WARFIGHTING FUNCTION. NETWORKS ARE PERVASIVE AND MUST BE SECURE AND INTEROPERABLE TO EFFECTIVELY MEET WARFIGHTER NEEDS. A SINGLE DESIGNATED APPROVAL AUTHORITY FOR NMCI AND ALL NETWORKS IN AOR WILL FACILITATE A UNIFIED CAPABILITY THROUGH AOR AND NETWORK CUTOVER. DAA SECURITY RESPONSIBILITIES REQUIRE MAINTENANCE OF DETAILED NETWORK SECURITY INFORMATION. THIS DATA MUST BE PROVIDED TO THE DAA TO ENSURE NETWORK RISK AND SECURITY MITIGATIONS ARE WELL UNDERSTOOD.
3. PROCEDURE: THE FOLLOWING REQUIREMENTS MUST BE COMPLETED 120 DAYS PRIOR TO CUTOVER (OR WITHIN 45 DAYS FROM THE DTG OF THIS MESSAGE FOR PREVIOUSLY AOR'D NETWORKS).
A. SPECIFIC DIRECTION FOR SITE ISSM AND LOCAL IA MANAGER (FORMERLY THE LOCAL DAA):
PROVIDE SSAA FOR EXISTING LEGACY NETWORK TO NETWARCOM, NAVY DAA. INCLUDE ARCHITECTURE AND NETWORK DRAWINGS, EXISTING IATO/ATO AND NETWORK RISK STATEMENT.
PROVIDE OLS REPORT/VULNERABILITY ASSESSMENT DATA FOR EXISTING LEGACY NETWORK/APPLICATIONS TO DAA. PROVIDE COPY OF SCM, PSQ AND RATIONALIZED APPLICATIONS LIST TO DAA.
PROVIDE IA MANAGER AND ISSM CONTACT INFORMATION TO GLOBAL ISSM.
COORDINATE WITH NMCI DAA TEAM (VIA POC ABOVE) TO CONDUCT SECURIFY SCANS ON LEGACY NETWORK.
PROVIDE LETTER OF ASSURANCE THAT CERTIFIES THE FOLLOWING:
(A) THERE ARE NO EXTERNAL OR "BACK DOOR" CONNECTIONS AND/OR LIST THOSE CONNECTIONS AUTHORIZED BY OFFICIAL APPROVED EXCEPTION THROUGH OPNAV WITH A COPY OF CORRESPONDENCE.
(B) THE NETWORK AND ALL CONNECTIONS ARE OPERATED IN COMPLIANCE WITH INFORMATION ASSURANCE (IA) PROGRAM POLICIES, THE UTN PROTECTION POLICY AND INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) PROGRAM.
FOR TRANSITION TO NMCI, COORDINATE WITH EDS TO PROVIDE COMPLETED ST&E IN ACCORDANCE WITH REF B, ENCLOSURE (3).

B. EDS CONTRACTOR IA TEAM:
PROVIDE SITE ISSC/ISSA CONTACT INFORMATION 120 DAYS PRIOR
TO CUTOVER TO SUPPORT COMMUNICATIONS BETWEEN THE SITE ISSM AND SITE ISSA.
PROVIDE SITE INSTALLATION AND UPGRADE PLANS TO PMW-161 IN
TIME TO SUPPORT TECHNICAL NETWORK ASSESSMENTS.
NMCI IATO/ATO PRIOR TO ACTIVATION OF TRANSPORT
BOUNDARIES, SERVER FARMS OR USER SEATS.
PROVIDE DAA WITH NMCI AOR IMPLEMENTATION SCHEDULE THAT
ADDRESSES AOR IMPLEMENTATION 60 DAYS IN ADVANCE.
C. UNDER THE DIRECTION OF THE DAA, IATT WILL COORDINATE CONDUCT OF SCANS
AND TECHNICAL NETWORK ASSESSMENTS, INCLUDING MITIGATION OF MAJOR
VULNERABILITIES, LEADING TO A RECOMMENDATION FOR IATO/ATO.

D. UPON COMPLETION OF ACTIONS OUTLINED ABOVE, THE NMCI DAA WILL:
PROVIDE DESIGNATION LETTERS FOR THE IA MANAGER AND ISSM.
UPON REVIEW OF DATA AND ASSESSMENT OF NETWORK RISK, PROVIDE IATO/ATO.//
BT
#8081
NNNN

D19. 021700Z MAY 03

021700Z MAY 03 COMNAVNETWARCOM NORFOLK VA

SUBJ/INTERIM APPROVAL TO OPERATE (IATO) THE UNCLASSIFIED
/NMCI TRANSITIONAL BOUNDARY TWO POLICY//

REF/A/DOC/SPAWAR PMW 161/04MAR2003/4A2-086/-/NOTAL//
REF/B/DOC/SPAWAR PMW 164/04MAR2003/4A2-085/-/NOTAL//
REF/C/DOC/NETWARCOM/04MAR2003//

NARR/REF A IS SPAWAR PMW 161 LTR OF RECOMMENDATION FOR B2
IMPLEMENTATION; REF B IS SPAWAR PMW 164 ENDORSEMENT OF THE
TRANSITIONAL B2 POLICY; REF C TRAFFIC POLICY MONITOR DEVICE
CAPABILITY REQUIREMENTS//

POC/BOB TURNER/CIV/NETWARCOM/LOC:NAB LCRK/TEL:(757)417-6776 EXT 2
/EMAIL:ROBERT.TURNER@NETWARCOM.NAVY.MIL//
POC/JOHN ROSS/LCDR/NETWARCOM/LOC:NORFOLK,VA/TEL:(757)417-6776 EXT 1
/EMAIL:JOHN.ROSS@NETWARCOM.NAVY.MIL//

RMKS/
1. THROUGH THE NMCI EFFORT, THE NAVY HAS EMBARKED ON AN AGGRESSIVE PROJECT FOR THE SEEMLESS NETWORKS INSIDE THE INTRANET AND A TRANSITIONAL DEFENSE-IN-DETH POSTURE DURING THE CUTOVER PROCESS
FROM LEGACY NETWORKS. IN SUPPORT OF THIS EFFORT, THE TRANSITIONAL BOUNDARY TWO FIREWALL POLICY WAS DEVELOPED.

2. THE NMCI OPERATIONAL DESIGNATED APPROVING AUTHORITY (DAA)GRANTS AN INTERIM APPROVAL TO OPERATE (IATO) FOR A PERIOD NTE ONE (1) YEAR ON THE UNCLASSIFIED NMCI NETWORK USING THE BELOW ENTERPRISE-WIDE B2 POLICY. THIS B2 POLICY SUPERSEDES ALL OTHER B2 POLICIES PREVIOUSLY RELEASED. ALLOWED PORTS AND PROTOCOLS (B2 POLICY LISTED WITHOUT RESTRICTIONS OR COMMENTS)

OUTBOUND (FROM THE NMCI ENCLAVE)

PORT	SERVICE	UDP	TCP
ALL	ALL	ALL	ALL

INBOUND (TO THE NMCI ENCLAVE FROM AOR'D LEGACY NETWORK)

PORT	SERVICE	UDP	TCP
25	SMTP		X
80	HTTP		X
102	X.400		X
137-138	NETBIOS	X	X
135,139	NETBIOS	X	
443	HTTPS		X
1433	SQL		X

3. THE NMCI TRANSITIONAL BOUNDARY TWO POLICY IS APPROVED WITH THE FOLLOWING CAVEATS:
A. ONLY THOSE LEGACY APPLICATIONS/DEVICES/SERVERS THAT HAVE BEEN REVIEWED BY THE NMCI CONNECTION APPROVAL REVIEW PANEL (NCARP) AND/OR APPROVED BY THE OPERATIONAL DAA ARE PERMITTED TO COMMUNICATE THROUGH B2.

B. ISF WILL CONTINUE TO PROVIDE A WEEKLY FORMAL WRITTEN STATUS REPORT UPDATING THE RESOLUTION OF ISSUES IDENTIFIED IN THE IATO TASK. REPORTS ARE TO BE PROVIDED TO PMW 161, CNO (N6143), AND NETWARCOM (N64).

C. ALL TROUBLE REPORTS AND RECOMMENDATIONS FOR CORRECTING VULNERABILITIES IDENTIFIED IN THE SECURITY TESTING AND EVALUATION (ST&E) AND REFERENCE (A) ARE TO BE ADDED TO THE IATO TASK LIST AND TRACKED UNTIL COMPLETION. ALL HIGH VULNERABILITIES MUST BE MITIGATED TO MEDIUM OR BELOW PRIOR TO CONNECTION TO NMCI.

D. AFTER COMPLETION OF OPERATIONAL TESTING, THIS IATO WILL BE REVISITED WITH ADDITIONAL REQUIREMENTS ADDED, IF NECESSARY.

E. PREMISE ROUTER INTERFACE BETWEEN LEGACY NETWORK AND LEGACY SERVICE PROVIDER CONFIGURED TO ALLOW ONLY THAT TRAFFIC REQUIRED FOR LEGACY SERVICES.

F. THE LEGACY NETWORK PREMISE (OR SEC RTR) CONNECTING TO EXTERNAL NETWORKS (I.E., NIPR, SMARTLINK, DREN) MUST IMPLEMENT AN ACL TO PREVENT TRAFFIC FROM ROUTING THROUGH THE LOCAL LEGACY TO B2 CONNECTION AND SUBSEQUENTLY NMCI. THIS CONFIGURATION SHOULD ALSO INCLUDE RULES TO PREVENT IP SPOOFING.

4. THE B2 POLICY WILL ALLOW ALL OUTBOUND-INITIATED CONNECTIONS TO THE LEGACY LAN IP SPACE AND WILL BE CONSTRAINED BY ACLS. INBOUND INITIATED CONNECTIONS FROM THE LEGACY LAN SHALL BE LOCKED DOWN TO SPECIFIC SERVER IP AND RESTRICTED TO THE MINIMUM NUMBER OF PORTS REQUIRED FROM THOSE LISTED IN PARA 2 ABOVE.

5. NETWORK SECURITY DEVICES ARE REQUIRED AT THE B2 INTERFACE AND THE LEGACY NETWORK. NETWORK SECURITY DEVICES ARE ALSO REQUIRED AT THE LEGACY NETWORK INNER ROUTER OF THE POP/FIREWALL, AS APPROPRIATE.

A. ONE OF THE SECURITY DEVICES WILL INCLUDE A TRAFFIC POLICY MONITOR. THE POLICY MONITOR MUST HAVE THE ABILITY TO UNWRAP "TUNNELED" TRAFFIC TO ACCURATELY REPORT PORT USAGE. THE POLICY MONITOR NEEDS TO HAVE THE CAPABILITIES IDENTIFIED IN REFERENCE (C).

B. NETWARCOM HAS REVIEWED AND APPROVED SECURIFY TO MEET THIS REQUIREMENT. OTHER PRODUCTS CAN BE USED WITH DAA APPROVAL.

6. DIR NMCI/PMO WILL ENSURE, PRIOR TO IMPLEMENTING THIS POLICY, THE FOLLOWING REPORTS ARE COMPLETED AND SUBMITTED TO THE DAA'S OFFICE FOR FINAL ASSESSMENT: DEPLOY NETWORK MONITORING DEVICES AND REPORT ALL UTN PROTECT POLICY NON-COMPLIANCE, A COMPLETE LIST OF LEGACY SYSTEM COMPONENTS AND ASSOCIATED HOST NAMES AND IP ADDRESSES CORRELATED TO PROGRAM OF RECORD NAMES, SITE SSAA REVIEW FOR ACCURACY, VERIFY IAVA COMPLIANCE ON THE LEGACY NETWORK AND A FIWC VULNERABILITY TEST RUN AS AN EXTERNAL PLAYER TO THE LEGACY NETWORK. THE INFORMATION ASSURANCE MANAGER (FORMERLY THE LOCAL DAA) IS REQUIRED TO CORRECT ALL DISCREPANCIES WITHIN THE SPECIFIED TIME FRAME DESIGNATED BY THE NMCI DAA.

7. IMPLEMENTATION OF THE B2 POLICY WILL START AT AOR AND CONTINUE WHILE LEGACY NETOWRK REQUIREMENT REMAINS. WITH THE EXCEPTION OF NMCI/IT21 B2 INTERFACE, ISF IS REQUIRED TO MODIFY ALL EXISTING LEGACY B2'S TO THIS BASELINE AS SOON AS POSSIBLE (REPORT WHEN ALL

MOD'S COMPLETE).

8. IN CONJUNCTION WITH AOR PLANS, PMW-161 IATT WILL ASSESS ALL B2 SYSTEMS REGARDLESS OF ITS PLACEMENT IN THE CYCLE.

9. A CONCERTED APPROACH BY THE DIR NMCI, ISF AND NAVY COMMANDS WILL WORK TO REMOVE ALL B2S FROM THE NMCI ARCHITECTURE BY 30 JUNE 2004. QQQQ

10. THIS CERTIFICATION APPROVAL IS GRANTED CONTINGENT ON THE CONTINUED ASSESSMENT BY THE NAVY CERTIFICATION AUTHORITY (PMW-161) THAT CONTINUED ACCEPTABLE PROGRESS IS BEING MADE.

11. ANY QUESTIONS OR COMMENTS CAN BE REFERRED TO THE POCS ABOVE.

12. THIS POLICY CANCELS ALL PREVIOUS NMCI BASELINE B2 POLICIES.//

Acronym List

ACL Access Control List
B2 Boundary Two
DAA Designated Approving Authority

FIWC Fleet Information Warfare Center
IATO Interim Approval To Operate
IAVA Information Assurance Vulnerability Alert

OLS ?
NCARP NMCI Connection Approval Review Panel

QLA Quick Look Assessment
QLAP Quick Look Assessment Panelist
QLAT Quick Look Assessment Team

SSAA System Security Authorization Agreement

ST&E Security Testing and Evaluation

SEC
RTR

UTN

The local DAA is now the “Information Assurance Manager.”

D20. 252230Z JUL 03

```
RAAUZYUW RUENAAA0974 2062230-UUUU--RHHMHAA.
ZNR UUUUU
R 252230Z JUL 03 ZYB PSN 892372E31
FM CNO WASHINGTON DC//N09//
TO RUCBCLF/COMLANTFLT NORFOLK VA
RHHMHAA/COMPACFLT PEARL HARBOR HI
RULSABC/USNA ANNAPOLIS MD
RULSFAN/COMNAVAIRSYSCOM PATUXENT RIVER MD
RUCOAHQ/COMNAVNETWARCOM NORFOLK VA
RUCTPOA/NETC PENSACOLA FL
RULSSEA/COMNAVSEASYSCOM WASHINGTON DC
RUENAAA/CNO WASHINGTON DC//N1//
RULSAMX/COMNAVSUPSYSCOM MECHANICSBURG PA
RULSOCA/CNR ARLINGTON VA
RUWDHFG/COMSPAWARSYSCOM SAN DIEGO CA
RUWDXGO/NAVPGSCOL MONTEREY CA
RULSADK/COMNAVFACENGCOM WASHINGTON DC
RUCCNOM/COMNAVRESFOR NEW ORLEANS LA
RULKSDF/COMNAVSECGRU FT GEORGE G MEADE MD
RULSDSA/DIRSSP WASHINGTON DC
RUCXONI/ONI WASHINGTON DC
RULSACL/NAVOBSY WASHINGTON DC
RUCCFLE/COMNAVMETOCCOM STENNIS SPACE CENTER MS
RUDFGHB/COMNAVNETSPAOPSCOM DAHLGREN VA
RHMFIUU/COMNAVNETSPAOPSCOM DAHLGREN VA
RULSWCB/NAVNETSPAOPSCOM DET WASHINGTON DC
INFO RUENAAA/ASSTSECNAV RDA WASHINGTON DC
RUEACMC/CMC WASHINGTON DC//C4//
RHMFIUU/CMC WASHINGTON DC//C4//
RUENAAA/CNO WASHINGTON DC//N6N7//
RUENAAA/DON CIO WASHINGTON DC
BT
UNCLAS //N02100//
MSGID/GENADMIN/CNO WASHDC/N09/-/JUL//
SUBJ/STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN
/NMCI//
REF/A/GENADMIN/CNO WASHINGTON DC/232208ZMAY2002//
AMPN/REF A, NAVADMIN 150/02, TARGETTED A 95 PERCENT REDUCTION IN
NAVY LEGACY APPLICATIONS AND AUTHORIZED DESIGNATED FUNCTIONAL AREA
MANAGERS (FAMS) TO DIRECT CONSOLIDATION, MIGRATION OR RETIREMENT OF
APPLICATIONS AND DATABASES WITHIN THEIR FUNCTIONAL AREAS AND ACROSS
ECHELON II ORGANIZATIONAL LINES.//
RMKS/1.  FUNCTIONAL AREA MANAGERS (FAMS) AND ORGANIZATIONS AT ALL
ECHELONS HAVE MADE GOOD PROGRESS TOWARD THE 95 PERCENT
REDUCTION.  AS OF 30 JUNE, MORE THAN 30,000 OF 37,287 IDENTIFIED
APPLICATIONS HAVE BEEN ELIMINATED.  REMAINING APPLICATIONS THAT ARE
CURRENTLY APPROVED FOR RETENTION/ALLOWED WITH RESTRICTIONS ARE
IDENTIFIED IN DON APPLICATION AND DATABASE MANAGEMENT SYSTEM
(DADMS), THE DESIGNATED AUTHORITATIVE SOURCE OF NAVY APPLICATIONS
DATA.  WORK CONTINUES TO REFINE THIS LIST AND DEVELOP MIGRATION
STRATEGIES.  THIS MESSAGE PUTS INTO PRACTICE THE
APPLICATION DECISIONS MADE TO DATE.
2.  ACTION:  ECHELON II COMMANDS ARE DIRECTED TO ENSURE THE
FOLLOWING:
A.  FOR COMMANDS COMMENCING NMCI CUTOVER AFTER 1 OCTOBER 2003, LIMIT
```

AUTHORIZED APPLICATIONS TO THOSE DESIGNATED AS FAM "APPROVED" OR "ALLOWED WITH RESTRICTIONS."
B. SHOULD APPLICATIONS ON THE DISAPPROVED LIST BE CONSIDERED MISSION CRITICAL, SUBMIT RECOMMENDATION AND JUSTIFICATION FOR PROPOSED WORKAROUND BY 8 AUGUST 2003 TO DIRECTOR, NAVY STAFF (DNS).
C. BY 15 AUGUST 2003, APPOINT A MIGRATION MANAGER TO LEAD THE MIGRATION STRATEGY AND IMPLEMENTATION PLAN.
D. BY 1 OCTOBER 2003, ELIMINATE DUAL DESKTOPS RETAINED SOLELY TO SUPPORT DISAPPROVED APPLICATIONS.
3. EXCEPTIONS TO THIS POLICY MUST BE REQUESTED, WITH ECHELON II CONCURRENCE, FROM THE APPROPRIATE FAM OR DNS.
4. AMPLIFICATION OF THE ACTIONS LISTED ABOVE CAN BE FOUND AT HTTPS://WWW.DADMS.NAVY.MIL.
5. RELEASED BY ADM WILLIAM J. FALLON, VCNO.//
BT

D21. 211902Z JUL 03

R 211902Z JUL 03 ZYB
FM CNO WASHINGTON DC//N09//
TO RUCBCLF/COMLANTFLT NORFOLK VA
RHHMHAA/COMPACFLT PEARL HARBOR HI
RULSABC/USNA ANNAPOLIS MD
RULSFAN/COMNAVAIRSYSCOM PATUXENT RIVER MD
RUCOAHQ/COMNAVNETWARCOM NORFOLK VA
RUCTPOA/NETC PENSACOLA FL
RUENMED/BUMED WASHINGTON DC
RULSSEA/COMNAVSEASYSCOM WASHINGTON DC
RUENAAA/CNO WASHINGTON DC//N1//
RULSAMX/COMNAVSUPSYSCOM MECHANICSBURG PA
RULSOCA/CNR ARLINGTON VA
RUWDHFG/COMSPAWARSYSCOM SAN DIEGO CA
RUWDXGO/NAVPGSCOL MONTEREY CA
RULSADK/COMNAVFACENGCOM WASHINGTON DC
RUCCNOM/COMNAVRESFOR NEW ORLEANS LA
RULKSDF/COMNAVSECGRU FT GEORGE G MEADE MD
RULSDSA/DIRSSP WASHINGTON DC
RUCXONI/ONI WASHINGTON DC
RULSACL/NAVOBSY WASHINGTON DC
RUCCFLE/COMNAVMETOCCOM STENNIS SPACE CENTER MS
RUDFGHB/COMNAVNETSPAOPSCOM DAHLGREN VA
RULSWCB/NAVNETSPAOPSCOM DET WASHINGTON DC
INFO RUENAAA/ASSTSECNAV RDA WASHINGTON DC
RUEACMC/CMC WASHINGTON DC//C4//
RHMFIUU/CMC WASHINGTON DC//C4//
RUENAAA/CNO WASHINGTON DC//N6N7//
RUENAAA/DON CIO WASHINGTON DC
BT
UNCLAS //N02100//
MSGID/GENADMIN/CNO WASHINGTON DC/N09/JUL//
SUBJ/NMCI PROGRESS//
RMKS/1. THIS MESSAGE REQUESTS YOUR IMMEDIATE AND ATTENTIVE ASSISTANCE TO FACILITATE NMCI INSTALLATION AND TO REDUCE LEGACY NETWORKS AND SOFTWARE APPLICATIONS.
2. THE IMPLEMENTATION OF THE NAVY MARINE CORPS INTRANET (NMCI) IS A TOP PRIORITY FOR THE DEPARTMENT OF THE NAVY AND REQUIRES EFFORT AT ALL LEVELS. NMCI IS A CRITICAL CAPABILITY IN ITS OWN RIGHT, AND IS AN ESSENTIAL ENABLER FOR KEY NAVY PROJECTS SUCH AS FORCENET AND SEA ENTERPRISE.
3. THE DON STRATEGIC GOALS ARE: PARTNER WITH THE NMCI PRIME CONTRACTOR, EDS, TO INSTALL ORDERED SERVICES BY 31 DEC 03 (WE CURRENTLY HAVE 295,000 SEATS ORDERED); REDUCE QUARANTINE SEAT RATIO TO UNDER 10%; AND NO DUAL DESKTOPS. (A QUARANTINE SEAT IS A COMPUTER STILL IN USE ON OUR OLD LEGACY NETWORKS WHICH SUPPORTS A REQUIRED APPLICATION THAT FAILED THE DON SOFTWARE STANDARDS. A DUAL DESKTOP IS A LEGACY DESKTOP RETAINED AS A MATTER OF PERSONAL PREFERENCE.)
4. COMMANDERS AT ALL ECHELONS CAN HELP TO ACHIEVE THESE OBJECTIVES BY THE FOLLOWING ACTIONS:
A. REDUCE APPLICATIONS. ONLY APPLICATIONS IDENTIFIED

AS APPROVED OR ALLOWED WITH RESTRICTIONS BY A FUNCTIONAL AREA MANAGER SHOULD BE RETAINED. (IMPLEMENTATION DETAILS TO BE PROVIDED SEPCOR)

B. ELIMINATE DUAL DESKTOPS.

C. PROVIDE ACCURATE AND TIMELY APPLICATION MAPPING DETAILS TO EDS. USE PROFILES WHERE POSSIBLE.

D. PROVIDE ACCURATE AND TIMELY ADMINISTRATIVE AND USER DATA TO EDS.

E. PROVIDE ACCESS FOR NMCI CONTRACTOR PERSONNEL TO FACILITIES FOR SURVEYS, BUILD OUT OF INFRASTRUCTURE, AND COMPUTER DEPLOYMENT. THIS INCLUDES ACCESS DURING NIGHT AND WEEKEND HOURS.

F. INCLUDE THE EDS SITE MANAGER ON COMMAND LEADERSHIP TEAMS.

G. TRAIN EMPLOYEES ON EFFICIENT USE OF THIS NEW SYSTEM AND THEIR RESPONSIBILITIES AS A MEMBER IN THE ENTERPRISE INTRANET. (SECURITY, EMAIL PROTOCOLS, PROBLEM NOTIFICATION, STORAGE LIMITS, ETC.)

5. ASSISTANCE IN ALL OF THESE ACTION AREAS IS AVAILABLE FROM THE NMCI OFFICE, THE NAVY OR USMC PROGRAM MANAGEMENT OFFICE, COMNAVNETWARCOM, USMC C4 AND THE EDS TRANSITION TEAM. WE NEED TO QUICKLY GET NMCI INSTALLATION BEHIND US SO WE CAN REAP THE BENEFITS OF THE SYSTEM.

6. RELEASED BY ADM WILLIAM J. FALLON, VCNO.//

BT

CNO WASH DC

D22. 071455Z AUG 03

R 071455Z AUG 03 NAVY DESIGNATED APPROVAL AUTHORITY ASSUMPTION

COMNAVNETWARCOM NORFOLK VA R 071455Z AUG 03 NAVY DESIGNATED APPROVAL AUTHORITY ASSUMPTION UNCLAS

R R 071455Z AUG 03 PSN 360671J23
FM COMNAVNETWARCOM NORFOLK VA
TO ALCND
INFO RUCBCLF/COMFLTFORCOM NORFOLK VA
RUENAAA/CNO WASHINGTON DC
ZEN/COMNAVNETWARCOM NORFOLK VA
BT
UNCLAS
ALCND 091-03
MSGID/GENADMIN/COMNAVNETWARCOM N00//

SUBJ/NAVY DESIGNATED APPROVAL AUTHORITY ASSUMPTION//

REF/A/DOC/CNO/02AUG2003//
AMPN/REF A IS OPNAV NOTICE 5230 DESIGNATING COMNAVNETWARCOM AS THE
PAGE 02 RUCOMFB8356 UNCLAS
DAA FOR ALL OPERATIONAL NAVY IT SYSTEMS AND NETWORKS.//
POC/ROBERT WHITKOP/CAPT/NETWARCOM DFN/LOC:NAB LITTLE CREEK VA
/TEL:757-417-6740/TEL:DSN: 537-6740
/EMAIL:ROBERT.WHITKOP(AT)NETWARCOM.NAVY.MIL//
POC/CATHY BABER/CIV/NETWARCOM N64/LOC:NAB LITTLE CREEK
/TEL:757-417-6767/TEL:DSN: 537-6767
/EMAIL:CATHY.BABER(AT)NETWARCOM.NAVY.MIL//

RMKS/1. PER REF A, NETWARCOM ASSUMES THE DUTIES OF DESIGNATED APPROVING AUTHORITY (DAA) FOR ALL OPERATING, GENSER, NAVY IT SYSTEMS AND NETWORKS. NETWARCOM WILL PUBLISH FURTHER GUIDANCE AND PROCEDURES RELATIVE TO THIS ASSIGNMENT WITHIN THE NEXT 60 DAYS.

2. ALL NAVY COMMANDS OPERATING AUTHORIZED NETWORKS SHALL CONTINUE TO ADHERE TO EXISTING DOD, DON AND OTHER OFFICIAL POLICY, GUIDANCE, DIRECTION AND PROCEDURES. NAVY COMMANDS SHOULD CONTINUE TO EVALUATE AND APPROVE OR DISAPPROVE ATO/IATO AND WAIVER REQUESTS FOR NETWORKS UNDER THEIR COGNIZANCE, ENSURING NETWARCOM IS KEPT APPRISED OF ALL DECISIONS AND IS PROVIDED A COPY OF ALL IATO AND WAIVER LETTERS AND SUPPORTING DOCUMENTATION VIA E-MAIL TO NETWARCOM N64.

3. THIS MESSAGE WILL REMAIN EFFECTIVE UNTIL SUPERCEDED.//
BT
#8356
NNNN
RTD:000-000/COPIES:

D23. 252230Z JUL 03

RAAUZYUW RUENAAA0974 2062230-UUUU--RHHMHAA.
ZNR UUUUU
R 252230Z JUL 03 ZYB PSN 892372E31
FM CNO WASHINGTON DC//N09//
TO RUCBCLF/COMLANTFLT NORFOLK VA
RHHMHAA/COMPACFLT PEARL HARBOR HI
RULSABC/USNA ANNAPOLIS MD
RULSFAN/COMNAVAIRSYSCOM PATUXENT RIVER MD
RUCOAHQ/COMNAVNETWARCOM NORFOLK VA
RUCTPOA/NETC PENSACOLA FL
RULSSEA/COMNAVSEASYSCOM WASHINGTON DC
RUENAAA/CNO WASHINGTON DC//N1//
RULSAMX/COMNAVSUPSYSCOM MECHANICSBURG PA
RULSOCA/CNR ARLINGTON VA
RUWDHFG/COMSPAWARSYSCOM SAN DIEGO CA
RUWDXGO/NAVPGSCOL MONTEREY CA
RULSADK/COMNAVFACENGCOM WASHINGTON DC
RUCCNOM/COMNAVRESFOR NEW ORLEANS LA
RULKSDF/COMNAVSECGRU FT GEORGE G MEADE MD
RULSDSA/DIRSSP WASHINGTON DC
RUCXONI/ONI WASHINGTON DC
RULSACL/NAVOBSY WASHINGTON DC
RUCCFLE/COMNAVMETOCCOM STENNIS SPACE CENTER MS
RUDFGHB/COMNAVNETSPAOPSCOM DAHLGREN VA
RHMFIUU/COMNAVNETSPAOPSCOM DAHLGREN VA
RULSWCB/NAVNETSPAOPSCOM DET WASHINGTON DC
INFO RUENAAA/ASSTSECNAV RDA WASHINGTON DC
RUEACMC/CMC WASHINGTON DC//C4//
RHMFIUU/CMC WASHINGTON DC//C4//
RUENAAA/CNO WASHINGTON DC//N6N7//
RUENAAA/DON CIO WASHINGTON DC
BT
UNCLAS //N02100//
MSGID/GENADMIN/CNO WASHDC/N09/-/JUL//
SUBJ/STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN /NMCI//
REF/A/GENADMIN/CNO WASHINGTON DC/232208ZMAY2002//
AMPN/REF A, NAVADMIN 150/02, TARGETTED A 95 PERCENT REDUCTION IN NAVY LEGACY APPLICATIONS AND AUTHORIZED DESIGNATED FUNCTIONAL AREA MANAGERS (FAMS) TO DIRECT CONSOLIDATION, MIGRATION OR RETIREMENT OF APPLICATIONS AND DATABASES WITHIN THEIR FUNCTIONAL AREAS AND ACROSS ECHELON II ORGANIZATIONAL LINES.//
RMKS/1. FUNCTIONAL AREA MANAGERS (FAMS) AND ORGANIZATIONS AT ALL ECHELONS HAVE MADE GOOD PROGRESS TOWARD THE 95 PERCENT REDUCTION. AS OF 30 JUNE, MORE THAN 30,000 OF 37,287 IDENTIFIED APPLICATIONS HAVE BEEN ELIMINATED. REMAINING APPLICATIONS THAT ARE CURRENTLY APPROVED FOR RETENTION/ALLOWED WITH RESTRICTIONS ARE IDENTIFIED IN DON APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS), THE DESIGNATED AUTHORITATIVE SOURCE OF NAVY APPLICATIONS DATA. WORK CONTINUES TO REFINE THIS LIST AND DEVELOP MIGRATION STRATEGIES. THIS MESSAGE PUTS INTO PRACTICE THE APPLICATION DECISIONS MADE TO DATE.

2. ACTION: ECHELON II COMMANDS ARE DIRECTED TO ENSURE THE FOLLOWING:
A. FOR COMMANDS COMMENCING NMCI CUTOVER AFTER 1 OCTOBER 2003, LIMIT AUTHORIZED APPLICATIONS TO THOSE DESIGNATED AS FAM "APPROVED" OR "ALLOWED WITH RESTRICTIONS."
B. SHOULD APPLICATIONS ON THE DISAPPROVED LIST BE CONSIDERED MISSION CRITICAL, SUBMIT RECOMMENDATION AND JUSTIFICATION FOR PROPOSED WORKAROUND BY 8 AUGUST 2003 TO DIRECTOR, NAVY STAFF (DNS).
C. BY 15 AUGUST 2003, APPOINT A MIGRATION MANAGER TO LEAD THE MIGRATION STRATEGY AND IMPLEMENTATION PLAN.
D. BY 1 OCTOBER 2003, ELIMINATE DUAL DESKTOPS RETAINED SOLELY TO SUPPORT DISAPPROVED APPLICATIONS.
3. EXCEPTIONS TO THIS POLICY MUST BE REQUESTED, WITH ECHELON II CONCURRENCE, FROM THE APPROPRIATE FAM OR DNS.
4. AMPLIFICATION OF THE ACTIONS LISTED ABOVE CAN BE FOUND AT HTTPS://WWW.DADMS.NAVY.MIL.
5. RELEASED BY ADM WILLIAM J. FALLON, VCNO.//
BT

D24. 011854Z AUG 03

R 011854Z AUG 03 PEO IT WASHINGTON DC(UC)

TO COMLANTFLT NORFOLK VA
COMPACFLT PEARL HARBOR HI
COMNAVNETWARCOM NORFOLK VA(uc)
COMNAVSEASYSCOM WASHINGTON DC(uc)
COMNAVAIRSYSCOM PATUXENT RIVER MD(uc)
COMNAVRESFOR NEW ORLEANS LA
COMNAVSUPSYSCOM MECHANICSBURG PA(uc)
COMSPAWARSYSCOM SAN DIEGO CA(uc)
COMNAVSECGRU FT GEORGE G MEADE MD
BUPERS MILLINGTON TN(uc)
BUMED WASHINGTON DC(uc)
NAVNETSPAOPSCOM DET WASHINGTON DC(uc)
COMNAVNETSPAOPSCOM DAHLGREN VA(uc)
COMNAVFACENGCOM WASHINGTON DC(uc)
ONI WASHINGTON DC
DIRSSP WASHINGTON DC(uc)
NETC PENSACOLA FL
COMNAVMETOCCOM STENNIS SPACE CENTER MS(uc)
CNR ARLINGTON VA(uc)
USNA ANNAPOLIS MD(uc)
NAVPGSCOL MONTEREY CA(uc)
NAVOBSY WASHINGTON DC(uc)
CC ASSTSECNAV RDA WASHINGTON DC(uc)
DON CIO WASHINGTON DC(uc)
CNO WASHINGTON DC
CMC WASHINGTON DC
CDR USJFCOM NORFOLK VAX(uc)
CDR USPACOM HONOLULU HI
PEO C4I AND SPACE SAN DIEGO CA(uc)
CG MARCORSYSCOM QUANTICO VA(uc)
COMMARFORLANT(uc)
COMMARFORPAC(uc)
PEO IT WASHINGTON DC(uc)

UNCLAS
MSGID/GENADMIN/PEO IT WASHINGTON DC/0040/AUG
REF/A/GENADMIN/CNO WASHINGTON DC/252230ZJUL2003/-/NOTAL
REF/B/GENADMIN/CNO WASHINGTON DC/232208ZMAY2003
NARR/REF A IS MSG STATING STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI. REF B IS NAVADMIN 150/02.
POC/ALLIE LAWAETZ/CONT/PEO IT WASHINGTON DC/-/TEL:703-685-5498 /EMAIL:ALLIE.LAWAETZ@NAVY.MIL
POC/RICHARD OPP/CIV/PEO IT WASHINGTON DC/-/TEL:703-685-5520 /EMAIL:RICHARD.OPP@NAVY.MIL

RMKS/1. REF A OUTLINES THE STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI. IN SUPPORT OF THIS STRATEGY, DIRECTOR NMCI PROVIDES THE FOLLOWING IMPLEMENTATION GUIDANCE FOR NMCI:
A. NMCI NETWORK: FOR SITES SCHEDULED TO COMMENCE NMCI SEAT INSTALLATION (CUTOVER) AFTER 1 OCTOBER 2003 FAM DISAPPROVED APPLICATIONS WILL NO LONGER BE LOADED ONTO NMCI AND THEY WILL NOT BE
APPROVED FOR RETENTION ON ANY LEGACY SEAT. CONSEQUENTLY SITES AND THEIR ECHELON II MUST WORK WITH FUNCTIONAL AREA MANAGERS TO ENSURE ANY DISAPPROVED APPLICATION REQUIRED TO MEET COMMAND MISSION HAS AN
APPROVED WAIVER. WAIVER PROCESS IS DEFINED IN REF A AMPLIFICATION AT HTTPS: WWW.DADMS.NAVY.MIL. FOR SITES CUTTING OVER AFTER OCTOBER 1, 2003, DISAPPROVED APPLICATIONS MAPPED TO USERS OR SEATS IN NET (NMCI ENTERPRISE TOOL) WILL BE AUTOMATICALLY FILTERED OUT BEFORE THE SEAT BUILD OUT TO STAGING PROCESS BEGINS. THE FAM STATUS IS REFLECTED IN ISF TOOLS AND ANY APPLICATIONS CHANGED FROM DISAPPROVED
TO APPROVED OR ALLOWED WITH RESTRICTIONS WILL BE UPDATED NIGHTLY FROM ISF TOOLS TO NET. THE CUT OFF POINT FOR DETERMINING WHAT APPLICATIONS GET LOADED WILL BE WHEN THE SITE PASSES THE SEAT BUILD OUT DATA TO ISF FOR STAGING. THIS TYPICALLY OCCURS 2-4 WEEKS BEFORE CUTOVER. ANY QUESTIONS REGARDING ISF TOOLS SHOULD BE DIRECTED TO CDR
JOE DUNDAS (EMAIL: JOE.DUNDAS@NAVY.MIL). ANY QUESTION REGARDING NET AND APPLICATION MAPPING SHOULD BE DIRECTED TO JILL COOKE (EMAIL: JILL.COOKE@NAVY.MIL). ANY QUESTIONS REGUARDING THE FAM PROCESS SHOULD BE DIRECTED TO CAPT SANDRA BUCKLES (EMAIL: SANDRA.BUCKLES@NAVY.MIL). TO REITERATE REFERENCE A POLICY, FOR ANY APPLICATION MARKED AS DISAPPROVED ON A SITE RATIONALIZED LIST IN ISF TOOLS THAT A COMMAND MUST HAVE, THE ECHELON II MUST SUBMIT A RECOMMENDATION AND JUSTIFICATION FOR A PROPOSED WORK AROUND TO THE
APPLICABLE FAM. ONLY FAM "APPROVED" OR "ALLOWED WITH RESTRICTIONS" APPLICATIONS THAT TECHNICALLY CANNOT OPERATE ON NMCI (FAIL LADRA/AIT
TESTING) ARE AUTHORIZED TO REMAIN ON QUARANTINE SEATS AND LEGACY NETWORKS. APPLICATIONS THAT BECOME APPROVED OR ALLOWED WITH RESTRICTIONS AFTER THE SITE CUT OFF POINT, DESCRIBED ABOVE, MUST FOLLOW THE NMCI RELEASE DEPLOYMENT PROCESS FOR TESTING, CERTIFICATION AND DEPLOYMENT INTO NMCI. THE NMCI RELEASE DEPLOYMENT
PROCESS IS FOUND IN THE NRDDG (NMCI RELEASE DEVELOPERS AND DEPLOYMENT GUIDE) AND CONSISTS OF THE STEPS A CDA OR APPLICATION OWNER MUST TAKE TO SUCCESSFULLY DEPLOY A RELEASE IN NMCI. ONCE THE RELEASE IS AVAILABLE FOR DEPLOYMENT, THE USER CAN REQUEST THE INSTALLATION OF THAT RELEASE VIA THE CTR/ACTR. THERE IS A COST FOR THIS TESTING AND DEPLOYMENT.
B. LEGACY NETWORK: THOSE ECHELON II'S WITH SITES CURRENTLY OPERATING DUAL DESKTOPS AND QUARANTINED SEATS MUST REVIEW THE CURRENT STATUS OF THEIR APPLICATIONS IN DADMS TO DETERMINE FAM

STATUS. SHOULD ANY QUARANTINED APPLICATIONS ON THE DISAPPROVED LIST BE CONSIDERED MISSION CRITICAL, ECHELON II MUST SUBMIT A RECOMMENDATION AND JUSTIFICATION FOR PROPOSED WORK AROUND AS DIRECTED IN REF (A) WITH A COPY TO NMCI DIRECTORS OFFICE (TIM.DONNELLY@NAVY.MIL) AND GAIN FAM APPROVAL OR ALLOWED WITH RESTRICTIONS STATUS. THE GUIDANCE FOR THIS PROCESS IS AVAILABLE AT WWW.DADMS.NAVY.MIL. IF THE QUARANTINED SEAT OR DUAL DESKTOP EXISTS SOLELY TO SUPPORT DISAPPROVED APPLICATIONS, IT SHOULD BE IDENTIFIED TO DIRECTOR NMCI AND THE LOCAL ISF TEAM FOR ELIMINATION. THE ECHELON II WILL ENSURE THESE DUAL DESKTOPS AND QUARANTINED SEATS ARE REPORTED

IN THE BIWEEKLY LEGACY WARFARE VTC WITH ASSOCIATED APPLICATIONS IDENTIFIED. AFTER 1 OCTOBER 2003, ALL FAM DISAPPROVED APPLICATIONS ON THE NETWARCOM MOST WANTED AND HIGH PRIORITY APPLICATION LISTING THAT DO NOT RECEIVE FAM APPROVAL WILL BE REMOVED FROM THE WORK LIST.

GO TO HTTP:/WWW.NMCI.NAVY.MIL/PRIMARY_AREAS/LEGACY_APPLICATIONS/LEGACY_APPLICATIONS_TRANSITION FOR FURTHER DETAIL.

2. COMMANDS ARE STRONGLY ENCOURAGED TO EXPEDITIOUSLY REVIEW THE FAM STATUS OF THEIR APPLICATIONS AND TAKE APPROPRIATE ACTION.

D25. 252230Z JUL 03

LAST UPDATED: 30 JULY 2003
AMPLIFYING INFORMATION FOR ACTION ITEMS IDENTIFIED IN R 252230Z JUL 03 CNO WASHINGTON DC//N09// GENADMIN MESSAGE, "STRATEGY FOR MANAGING NAVY APPLICATIONS AND DATABASES WITHIN NMCI".
BOLDED SECTIONS BELOW CONTAIN THE WORDS AND PARAGRAPH MARKINGS FROM THE ACTUAL MESSAGE.

"2.A. FOR COMMANDS COMMENCING NMCI CUTOVER AFTER 1 OCTOBER 2003, LIMIT AUTHORIZED APPLICATIONS TO THOSE DESIGNATED AS FAM 'APPROVED' OR 'ALLOWED WITH RESTRICTIONS.'"

Amplification:
This restriction applies to applications loaded on Navy NMCI seats, remaining unclassified legacy networks (already in AOR with NMCI and those yet to be AOR'd), and NMCI quarantine seats. Commands are responsible for verifying within DADMS the status of their desired applications prior to entering their requests in ISF Tools. Commands that have already ordered their applications may have to amend their order, if their cutover is scheduled to commence after 1 October 2003. If the application is "Allowed with Restrictions", note that the FAM specified restrictions may prohibit use of the application at the site in question or prohibit use for a specific purpose.

"2.B. SHOULD APPLICATIONS ON THE DISAPPROVED LIST BE CONSIDERED MISSION CRITICAL, SUBMIT RECOMMENDATION AND JUSTIFICATION FOR PROPOSED WORKAROUND BY 8 AUGUST 2003 TO DIRECTOR, NAVY STAFF (DNS). "

Amplification:
By 8 August 2003, review the list of applications associated with your command in DADMS for which the FAM Status is "Approved" or "Allowed with Restriction". If there are any applications that you evaluate as the only current, viable option for supporting a critical mission, and those applications do not appear as approved or allowed, the first recourse is to submit a waiver to the appropriate FAM through DADMS. The key to a successful waiver is a strong, detailed justification with an explicit link to critical processes.

If a "FAM Disapproved" application is considered to be an authoritative source of data, which feeds other critical applications or processes, this may be justification for submitting a DADMS waiver for the disapproved application. Identifying such applications requires in-depth process knowledge (i.e., the ability to detail required data flows between/among applications). There are examples where key data exchanges are accomplished through informal, and/or manual methods.

If all reasonable efforts to obtain FAM approval have been exhausted via the waiver process and you feel that an appeal of the FAM decision is warranted, submit that appeal to OPNAV CIO at OPNAVCIO@navy.mil. The basis of the appeal should be documented in the "Echelon II Appeal of FAM Waiver Disapproval" Form (Attachment A). If the FAM has designated a preferred, alternative application, ensure that the appeal clearly articulates the reason that the preferred alternative is not acceptable. The nominal time for resolution of such appeals will be 10 working days. POC for appeals is CDR Mark Murphy (mark.a.murphy@navy.mil, 703-602-5131).

"2.C. BY 15 AUGUST 2003, APPOINT A MIGRATION MANAGER TO LEAD THE MIGRATION STRATEGY AND IMPLEMENTATION PLAN"

Amplification:
At a minimum, "Migration Managers" should be designated for each Echelon II Command. Migration Managers will coordinate the planning and execution of all application migration for their Echelon II and all subordinate commands. In some cases it may be necessary to designate an "Application Migration Manager" for individual applications. The Echelon II Migration Manager will coordinate with the FAMs and their respective Echelon II FAM representatives. This will most likely be a full time effort as it is anticipated that thousands of applications will be migrated over the next several years. Submit Migration Manager contact information (Name, rank, office code, phone number, email address) to CAPT Sandra Buckles at sandra.buckles@navy.mil.

"2.D. BY 1 OCTOBER 2003, ELIMINATE DUAL DESKTOPS RETAINED SOLELY TO SUPPORT DISAPPROVED APPLICATIONS."

Amplification:
If an application is the only practical option to support a mission critical process / function, but it cannot be certified for operation on NMCI, then it must be "Allowed with Restrictions" by the applicable FAM if it is to continue to be used as justification for the retention of a legacy seat. FAMs will restrict use of the application to the greatest extent that is practical.

"3. EXCEPTIONS TO THIS POLICY MUST BE REQUESTED, WITH ECHELON II CONCURRENCE, FROM THE APPROPRIATE FAM OR DNS."

Amplification:
Commands requesting waivers for a "Disapproved" application must submit an ACCURATELY completed questionnaire in DADMS (https://www.dadms.navy.mil) within 5 working days of the initial waiver request. Both a waiver request and a completed DADMS questionnaire are prerequisites to FAM processing. A questionnaire is not considered complete until all asterisked questions/data fields in all six sections are ACCURATELY filled in, and the appropriate UIC, CDA and Echelon II signatures have been entered. (CDA signature is typically not required for COTS)). Once the waiver form and application questionnaire are completed in DADMS, FAMs have 5 working days to process the submitted waiver. If the questionnaire is placed in the "insufficient info" category of DADMS, the application has not met the minimum requirements for consideration by the FAM, cannot be processed, and will be disapproved by the FAM after 5 working days. No FAM response after 5 working days with an ACCURATELY completed waiver form and application questionnaire in DADMS, implies approval of the waiver for the application as "Allowed with Restrictions" (only "Allowed with Restriction" for the command submitting the waiver) for a period not to exceed 120 days. To preclude a delay in NMCI seat rollout the applicable FAM and/or Echelon II Command may authorize a legacy desktop for duration not to exceed 120 days.

ATTACHMENT A

Echelon II Appeal of FAM Waiver Disapproval

Date:	
Submitting Echelon II:	
Point of Contact at Submitting Echelon II	
Name:	Title:
Phone:	Email:
Application Information	
Application Name:	Type (COTS/GOTS):
Manufacturer/CDA:	Functional Area:
DADMS ID:	ISF Tools ID:
Reason for Appeal	
Describe the critical process that this application supports:	
What is the impact on your mission if this application is not approved for use on NMCI?	
Why did the FAM disapprove the waiver for this application?	
What is the justification for this appeal?	

Submit this form to OPNAVCIO@navy.mil
Appeal POC is CDR Mark Murphy (703-602-5131, mark.a.murphy@navy.mil)

ATTACHMENT A

APPENDIX E – NMCI APPLICATION RULESET (REVISED)

V2.96

NMCI Ruleset is also posted on NADTF website
http://cno-n6.hq.navy.mil/navcio/leg_apps.htm

Ruleset Is A Reference	The NMCI Rule set is designed to be a summary of the information contained in the Legacy Applications Transition Guide (LATG) and the NMCI Release Development and Deployment Guide (NRDDG). Should questions arise from the use of the Rule Set, the user should refer to the LATG or NRDDG, or contact the Navy Applications Data Base Task Force (NADTF) for clarification.

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 1	**Windows 2000 (W2K) Compatible**	The candidate application is not compatible with the Windows 2000 operating system. This means it will either not run properly under Windows 2000 or that it interferes with the normal functionality of the operating system.	Waivers will not be considered for this ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA and owning FAM to upgrade the application to Windows 2000 compatibility or it should be replaced by another that is Windows 2000 compliant. Once a compliant version is identified it will be submitted for NMCI testing and certification. Applications that cannot be corrected will be quarantined for no more than 6 months and then will be removed from the quarantine workstation. The application will then be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel the RFS and unlink the application from their UICs in the ISF Tools database.	**FAIL**
RULE 2	**NMCI Group Policy Object (GPO) Compatible**	The candidate application is not compatible with the Group Policy Object (GPO) security rules for the workstation. For instance, if the candidate application requires full control of the c:\winnt folder in order to run, this violates NMCI enterprise policy governing connection to the NMCI network.	Waivers will not be considered for this ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA, owning FAM, ISF, and NMCI DAA to correct the GPO failure. NETWARCOM and ISF will provide the technical data detailing cause of the failure. Once the GPO failure is resolved, the application will be re-tested. GPO Policy changes may be requested from the NMCI DAA. Applications that cannot be corrected will be quarantined for no more than 6 months and then be removed from the quarantine workstation. If the application cannot be corrected, it must be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	**FAIL**

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 3	**No Duplication of Gold Disk Software or Services**	The candidate application or service duplicates the functionality of the NMCI Standard Seat Services ("Gold Disk") applications. (Example: Word 2000 replaces all versions of WordPerfect and other word processors. Windows Media Player, Real Player, and QuickTime replace all other audio/video players).	Claimant should discard the current application and use the application or service that exists on the Gold Disk. This application is not eligible for quarantine. Waiver requests may be submitted to the appropriate FAM via the DADMS Waiver Questionnaire, but approvals will only be given if Claimant can show degradation to the mission, and can show that they cannot afford to upgrade to authorized NMCI software or services. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database	KILL UNLESS WAIVER AUTHORIZED
RULE 4	**Comply with DON/NMCI Boundary 1 and 2-Policies**	The ISF and NMCI DAA have determined, through testing, that the candidate application is non-compliant with NMCI Boundary firewall policies (violation of B1/B2 rulesets).	Claimant must resolve violation with the application POR/CDA, owning FAM, ISF, and NMCI DAA to determine how to correct the Boundary policy violation. Once the policy violation is resolved, the application will be re-tested. Waivers will not be considered for this ruleset. Requests to operate a non-compliant system for B1 Firewall policy violations are managed by OPNAV and B2 policy changes are reviewed and managed by the NMCI DAA. B2 boundary issues may be resolved by moving servers into NMCI enclave. Applications that cannot be corrected will be quarantined for no more than 6 months and will then be removed from the quarantine workstation. These applications will then be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	FAIL
RULE 5	**No Setup, Installation, Uninstallation, Update and Auto update Tools or Utilities**	The candidate application is actually a tool or utility used to load and remove applications. Since ISF conducts all application installation and removal in NMCI, these types of files will not be authorized in ISF Tools DB or on the Rationalized List. Examples include Setup, Install, Uninstall, Launch, Autolaunch, Run, AutoRun, Updater, AutoUpdater or other installation-type Applications.	ISF will not test this application and waivers will not be considered. These types of applications will be removed from tracking and the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	KILL

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 6	**No Games**	The candidate application is a "game" as defined by PEO-IT, NAVY IO and the PMO, and is prohibited on the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine the game is required for mission accomplishment (Modeling, Simulation, or Training). The Claimant must submit a waiver request to the appropriate FAM via the DADMS Waiver Questionnaire. Applications already approved by the M&S and/or Training FAM will not require waivers. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	**KILL UNLESS WAIVER AUTHORIZED**
RULE 7	**Restrictions on Freeware or Shareware**	The candidate application is "Freeware" or "Shareware" as defined by PEO-IT, NAVY IO or the PMO, and significant restrictions are imposed for applications using shareware or freeware in the NMCI environment. Enterprise life cycle support and licensing issues accompany most "Freeware and Shareware" and are the responsibility of the CDA or sponsoring FAM.	The candidate application either employs "freeware and/or shareware" in the construct of a GOTS application or is a "freeware and/or shareware" application which is sponsored by a CDA or a FAM. Enterprise life cycle support and licensing must be provided by the responsible CDA or the responsible FAM prior to the submission of freeware/shareware for NMCI testing. Waivers for freeware and shareware must be submitted by the POR/CDA or FAM and be approved by the NADTF prior to NMCI testing using the DADMS Waiver Questionnaire. The waiver request must include the CDA's/FAM's commitment for enterprise lifecycle and licensing support. The NADTF will coordinate the waiver request with the NMCI DAA. Freeware/shareware applications will not be installed on quarantine networks and/or dual desktop configurations. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. The Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	**KILL UNLESS WAIVER AUTHORIZED**
RULE 8	**No Beta/Test Software (Authorized on S&T Seats Only)**	The candidate application is a "beta" or a "test" version, as defined by the PEO-IT, NAVY IO, or the PMO and is therefore prohibited in the NMCI environment.	ISF will not test this application and a waiver will not be considered. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database, and not included on any Rationalized List, nor should an RFS be submitted. If the Beta or Test Software is critical for mission accomplishment, the Claimant may purchase an S&T Seat. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	**KILL**

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 9	**No Application Development Software (Authorized on S&T Seats Only)**	The candidate application is "application development" software, as defined by either PEO-IT, NAVY IO or the PMO, and therefore is not authorized on standard NMCI Seats. The candidate application would be permitted if operated on an NMCI ordered Science and Technology (S&T) Seat. Application Development Software will not be tracked on the Rationalized List in the ISF Tools Database nor submitted for certification.	ISF will not test this application and a waiver will not be considered. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database, and not included on any Rationalized List, nor should an RFS be submitted. If the application development software is critical for mission accomplishment, the Claimant may purchase an S&T Seat, which allows for the installation of development software. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	**KILL**
RULE 10	**No Agent Software**	The candidate application is "agent" software, as defined by PEO-IT, NAVY IO or the PMO. Agents in the NMCI environment are controlled by ISF. No other candidate agents are allowed in the NMCI environment. Agents are code modules installed on client machines (or network devices) often used to poll, monitor, and collect system or network node performance data and send it to management consoles elsewhere on the network. These present a security risk to NMCI. Network monitoring and management are the responsibilities of the ISF.	These types of applications will be removed from tracking in the Legacy Applications Rationalized List and the ISF Tools Database. These applications will not be considered for waivers. No polling and monitoring of legacy networks and systems and collecting of data is authorized from within NMCI Polling, monitoring and collecting system and network data from legacy networks and systems is still authorized from legacy network assets only. Viewing collected legacy network or system data from NMCI seats is allowed using non-agent software.	**KILL**
RULE 11	**Gold Disk Compatible**	The application software is not compatible with the standard "Gold Disk" software and services. This means that the candidate application does not interact properly with one or more of the set of applications or services that have been selected to be installed on all NMCI seats.	Waivers will not be considered for this ruleset. The application is quarantined for no more than 6 months and then it is removed from the quarantine workstation. The application will be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel the RFS and unlink this application from their UICs in the ISF Tools database. Claimants and POR/CDA must work with the ISF to determine Gold Disk compatibility issues. The POR/CDA then works with the owning FAM to upgrade, replace or retire the application. Once a compliant version is identified it must be submitted for NMCI testing.	**FAIL**

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 12	**No Peripherals, Peripheral Drivers or Internal Hardware**	The candidate submission is a component (driver or hardware helper app) dealing directly with allowing a peripheral piece of hardware to function (Scanner, Printer, Plotters, Chartmakers, CDRW drive, ZIP or JAZ drive, Camcorder, PDA, etc). This enabling software must be tracked with the hardware on the Peripherals list and not entered into ISF Tools Database or listed on the Rationalized List. Internal hardware and the associated driver are not permitted within NMCI.	Peripherals and enabling software (drivers) are not entered into the ISF Tools Database nor placed on the Rationalized List. Peripherals and Peripheral Drivers are tracked separately from the ISF Tools Database and the Rationalized List, and are included in the Peripheral Drivers List. The Peripheral Drivers List is submitted to the ISF on-site for processing. If the driver is part of a bundled software package, that bundled package is handled like an application. The bundled package is entered into the ISF Tools Database, placed on the Rationalized List, and tested by the ISF.	KILL
RULE 13	**No personal, non-mission, or non-business related software**	The candidate application is "personal, non-mission, or non-business related", and is therefore prohibited in the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine that this application is required for mission accomplishment. These applications will not be installed on a quarantine workstation. The claimant must submit a waiver request to the appropriate FAM via the DADMS Waiver Questionnaire. If the waiver is not approved or submitted, the application must be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	KILL UNLESS WAIVER AUTHORIZED
RULE 14	**8/16-Bit Applications**	8-bit and 16-bit applications may migrate into the NMCI environment with an approved FAM waiver and a realistic migration plan that identifies a path to 32-bit status. Applications without approved waivers will not migrate to NMCI or Quarantined environments. Identification of an application as 8-bit or 16-bit does not stop the testing process (PIAB and LADRA). The application must pass all other rules and testing for 8-bit and 16-bit waivers to be approved.	Claimant and/or POR/CDA will submit a waiver immediately to the appropriate FAM via the DADMS Waiver Questionnaire requesting the 8/16-bit application migrate into NMCI. The request must include a detailed migration plan to get 8/16-bit application to 32-bit or web application status. ISF must process and certify the application while the waiver is being submitted. ISF will deploy the application while the waiver is being processed. If the waiver is not authorized (disapproved), the application is quarantined for no more than 6 months, then removed from the quarantine workstation and archived in the ISF Tools database. Applications for which a waiver was not submitted will not be quarantined, and will be removed from the Rationalized List and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	PROCESS AND CERTIFY APPLICATION DEPLOYMENT WHILE WAIVER IS AUTHORIZED

Definitions	
Fail	Fail is defined as violating the NMCI Application Ruleset by failing to successfully meet compliance or usability testing standards. These applications are flagged as Quarantined and will operate on a quarantined workstation in the legacy environment until the Ruleset violation or test failure is resolved or a waiver to operate within NMCI has been submitted and approved.
Kill	Kill is defined as violating the NMCI Application Ruleset. The application is not compliant with the rules and standards for applications within NMCI as set by the Navy IO. These applications will not be flagged as Quarantined and will be removed from the Rationalization List and ISF Tools database, unless a waiver to the rule is submitted and approved.
Application Development Software	Any software that generates or allows the user to create programming code which compiles into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.
Agent Software	Any software that polls, monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.

APPENDIX F – CLASSIFIED LEGACY APPLICATIONS TRANSITION PROCESS

1.0 — CNO GUIDANCE

This document represents a complete baseline overview of the Classified Legacy Applications Transition Process. It is intended for Navy Marine Corps Intranet (NMCI) customers involved in the transition of Classified Legacy Applications. Both Electronic Data System (EDS) and Government program management personnel have worked in close cooperation to design the processes and procedures described here. All CNO guidance, Naval messages, and requirements addressed in the Legacy Applications Rapid Certification Phase, Section 1.0, apply in the processing of Classified Legacy Applications.

2.0 — OVERALL LEGACY APPLICATIONS TRANSITION PROCESS

An overview of the NMCI Legacy Applications Transition Process is provided in the Legacy Applications Rapid Certification Phase, Section 4.0. The classified legacy applications process does not differ significantly from the processing of unclassified applications in the LA Rapid Certification Phase, except where stated below.

The Certification Phase includes Assumption of Responsibility (AOR), Seat Cutover (start), and Seat Cutover (end). The Risk Mitigation Phase begins when Seat Cutover is complete and continues until transition is complete. These distinct and comprehensive processes contain the main pieces of information crucial to transition success and are explained in greater detail in the main sections of this guide. Within the Classified Legacy Applications Transition Process, customers will become involved with:

- The creation of a Classified Rationalized List of applications.
- The submission of Classified Requests for Service (CRFSs) and application media to EDS.
- Functional Testing of the application.
- Assisting the EDS with IA Compliance Assessment.

Within the Risk Mitigation Phase, information regarding system documentation, transition planning, and accreditation will be required. This guide does not address the Risk Mitigation Phase.

Figure F-1 depicts an overview of the legacy application transition. It shows the distinction between the Rapid Certification and Risk Mitigation Phases. Again, this process does not differ significantly from the processing of unclassified legacy applications. It breaks down the Rapid Certification Phase into smaller processes that describe the "life of a transitioning application." Each of these smaller processes, the information needed for each, and the key people involved with each, are covered in the main sections of this guide.

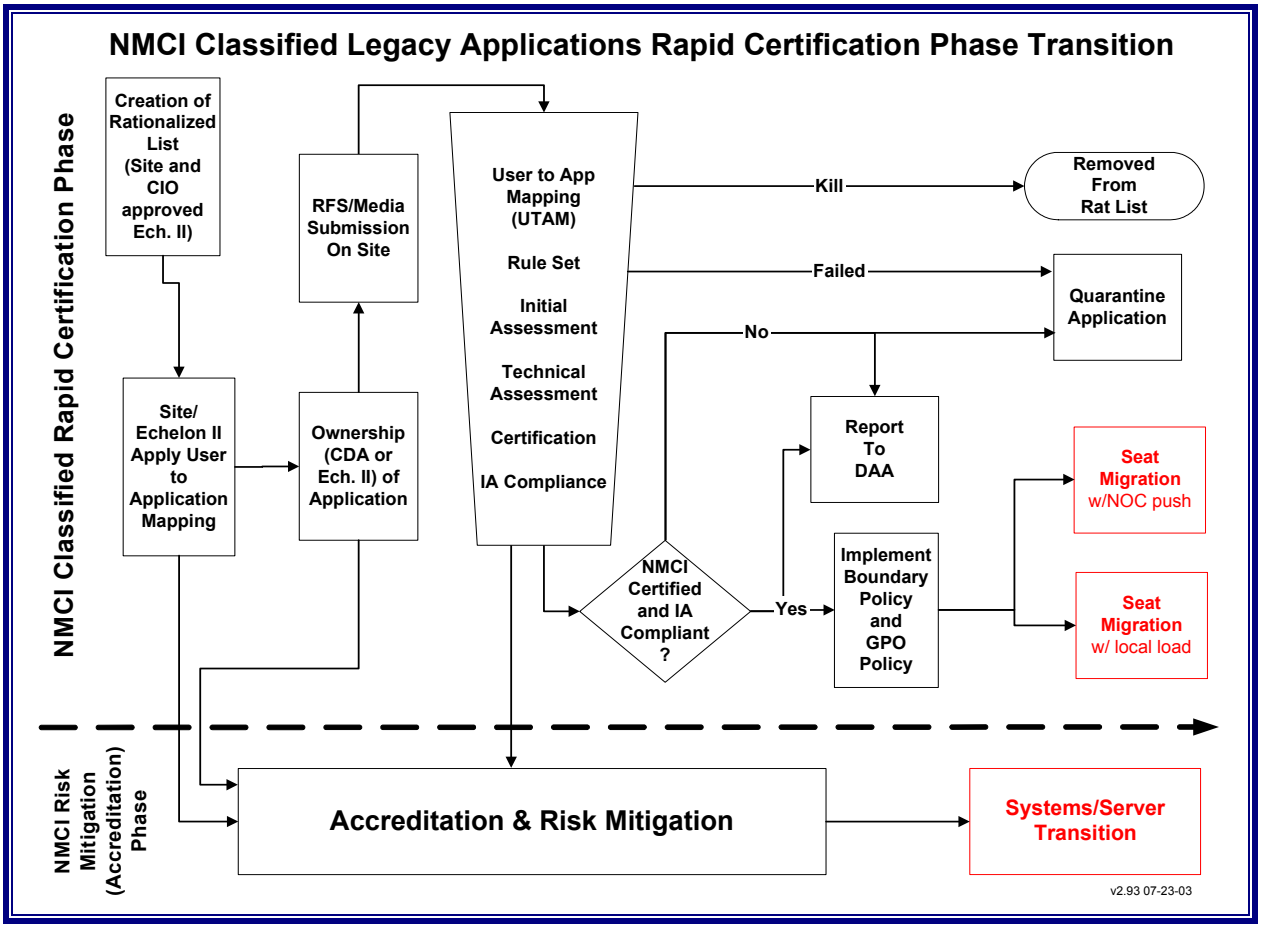


Figure F-1. NMCI Classified Legacy Applications Rapid Certification Phase Transition

3.0 —CLASSIFIED LEGACY APPLICATIONS TRANSITION PROCESS (RAPID CERTIFICATION PHASE)

Figure F-2 depicts the detailed Classified Legacy Applications Transition Process from start to finish. Notice the legend at the bottom right side of Figure F-2. The colors in the legend correspond to ownership of primary responsibility for completion of the process. For example, the "Media Submission" box is blue, and represents a Government/site responsibility for completion. Note that many of the processes are tan, indicating a joint responsibility for completion shared by the EDS and the Government.

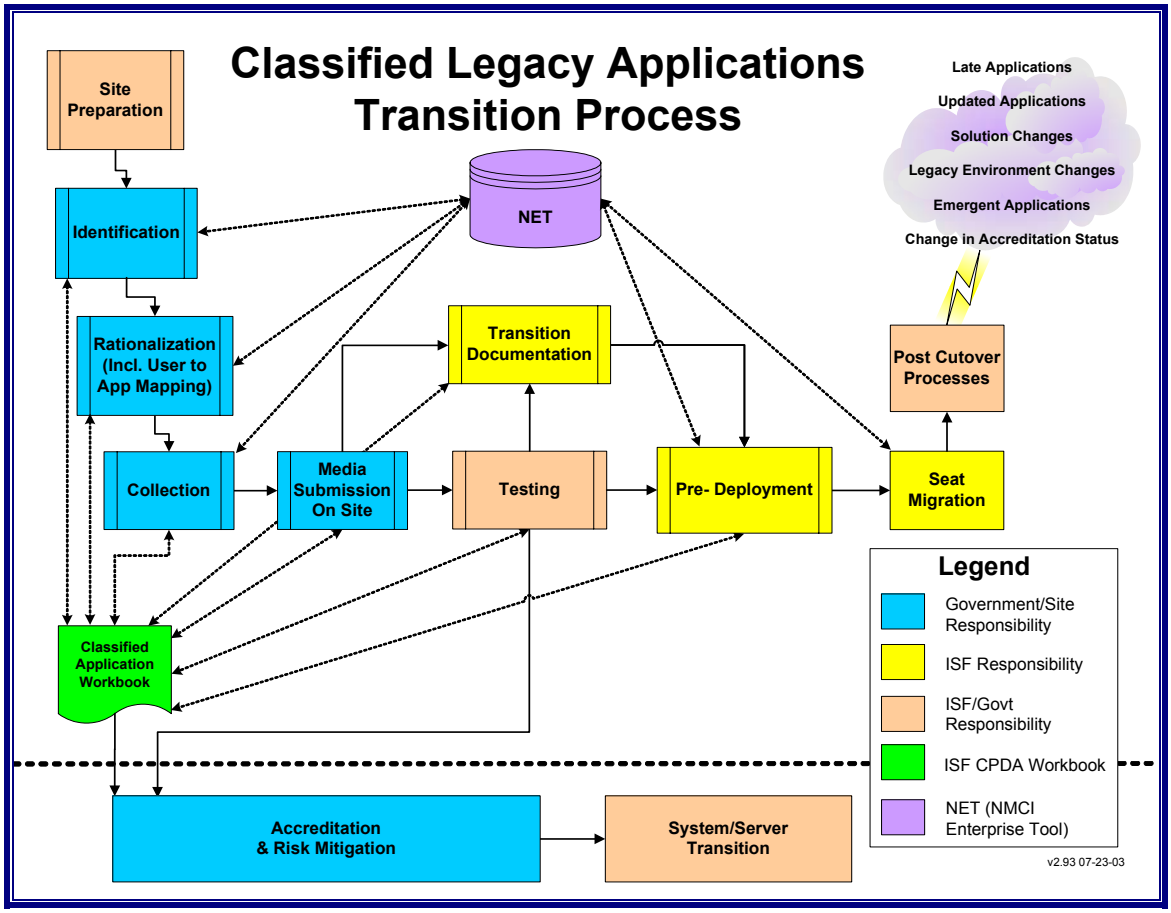


Figure F-2. Classified Legacy Applications Transition Process

The use of the ISF Tools Database is the main difference between the processing of unclassified and classified legacy applications. The Unclassified Rapid Certification Phase (for unclassified legacy applications) utilizes the ISF Tools Database, while the Classified Legacy Applications Transition Process maintains manual tracking of the Classified Legacy Applications Rationalized Lists, Workbooks, and CRFSs.

The overall goal of the Rapid Certification Phase and the Classified Legacy Applications Transition Process is to work with the EDS to ensure that the right applications are available to the NMCI seats of the right people at the right time, to ensure completion of the mission and business of the DON. From the customer's perspective, this means many things, including:

- Understanding who uses particular applications at the site.
- Understanding what version(s) of an application are in use at the site.
- Communicating with EDS and Program Management Office (PMO) personnel to help them understand the applications.
- Communicating with appropriate Echelon II personnel as lists of needed applications are reviewed.
- Making the resources available to accomplish the processes.

3.1 Classified Site Preparation

Figure F-3 depicts the details of site preparation from the NMCI customer perspective. The activities are designed to get a site ready to start the transition process well before any contractor or government program management personnel are involved. The major difference here is the requirement for a secure facility/storage, custody, and personnel clearances. This is the vital piece in the whole Classified Legacy Applications transition process and its importance cannot be overstated. To that end, the site Information System Security Manager/Officer (ISSM/O) is the one individual uniquely placed to ensure that all site security requirements and arrangements are carefully planned and coordinated well in advance of the arrival of any EDS transitioning teams. In association with the LAPOC the Command/Site ISSM/O, Site DAA, and EDS SM will ensure that the following areas are properly addressed and coordinated:

- Obtain secured classified storage for classified documentation.
- Obtain secure classified workspace for classified application processing.
- Acquire CRFS from EDS NMCI website or this Appendix.
- Determine facility requirements for Classified PIAB or Classified Legacy Application Deployment Readiness Activity (CLADRA) seat configuration.
- Acquire local SIPRNET Interim Authority to Connect (IATC) for CPIAB.
- Review, Accept and Assign facilities.

Customers should contact the Site Transition Execution Manager (STEM) Management Office (SMO) at the Navy NMCI PMO, SPAWAR PMW-164 for specific questions on Classified Legacy Application transition issues. The E-mail address for the SMO is clasrat@spawar.navy.mil.

Customers must determine the best location at their site for a secure test area in which to place a Classified Point of Presence (PoP)-In-A-Box (CPIAB) or NMCI Test Seat. The CPIAB is a "mini-NMCI environment" used by the EDS to understand application characteristics. The NMCI Test Seat is an actual NMCI seat used when the Classified NMCI base infrastructure is in place.

This is important because it gives EDS and Information Assurance (IA) personnel a way to understand the ports and protocols that applications use when they communicate. Deployment of a CPIAB or Classified NMCI Test Seat to a site comes later in the transition process, but a wise site prepares facilities makes network access arrangements, and understands power requirements in advance of its arrival. Further information on the CPIAB and Classified NMCI Test Seat can be obtained by contacting the EDS Site Manager (SM) and Site Solutions Engineering Team.

Once the preparatory steps have been completed, the site goes to the Identification and Rationalization processes.

3.2 Classified Application Identification and Rationalization

Once again the major differences between the Unclassified Legacy Application Transition process and the Classified Legacy Applications Transition Process are the use of manual submission and tracking methods of the:

- Classified Legacy Applications Rationalized List
- Classified Legacy Applications Workbook
- CRFS
- Certification Letter

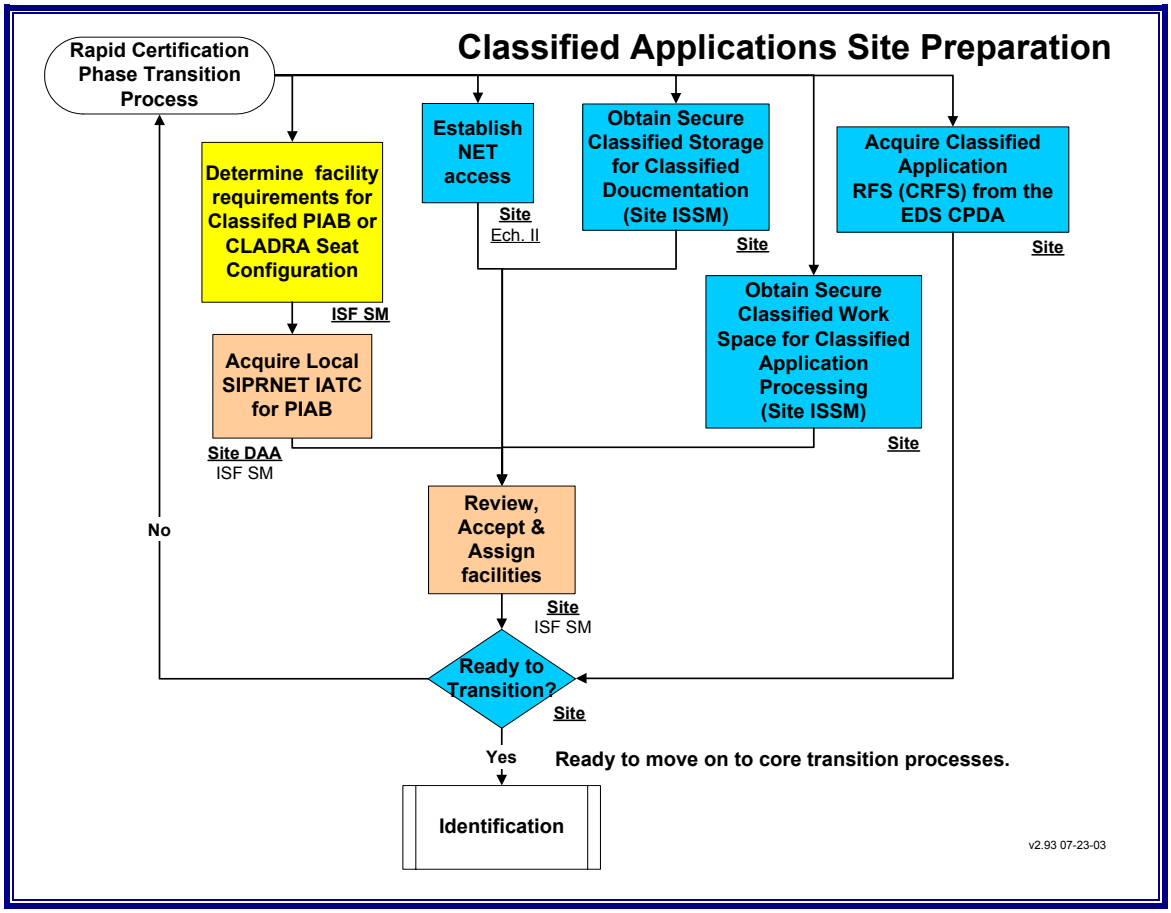


Figure F-3. Classified Applications Site Preparation

Figure F-4 and Figure F-5 depicts the Classified Identification and Rationalization steps.

3.2.1 Classified Application Identification

The Classified Legacy Applications Identification process differs from the unclassified process in the use of the ISF Tools Database. Once the classified applications are identified, they are entered into the Classified Legacy Applications Rationalized List template, creating the Raw Classified Applications List.

The Classified Legacy Applications Rationalized List format, in Microsoft Excel, can be found on the EDS NMCI website at http://www.nmci-isf.com/transition.htm.

See Figure F-4 for more details of the Classified Legacy Applications Identification process. The remaining steps of the Classified Identification Process are the same as those depicted in the unclassified processes of this guide.

Customers must identify their Legacy Applications on time. Lateness jeopardizes inclusion in Seat Cutover. See Appendix C of this guide for more information on Late Submission.

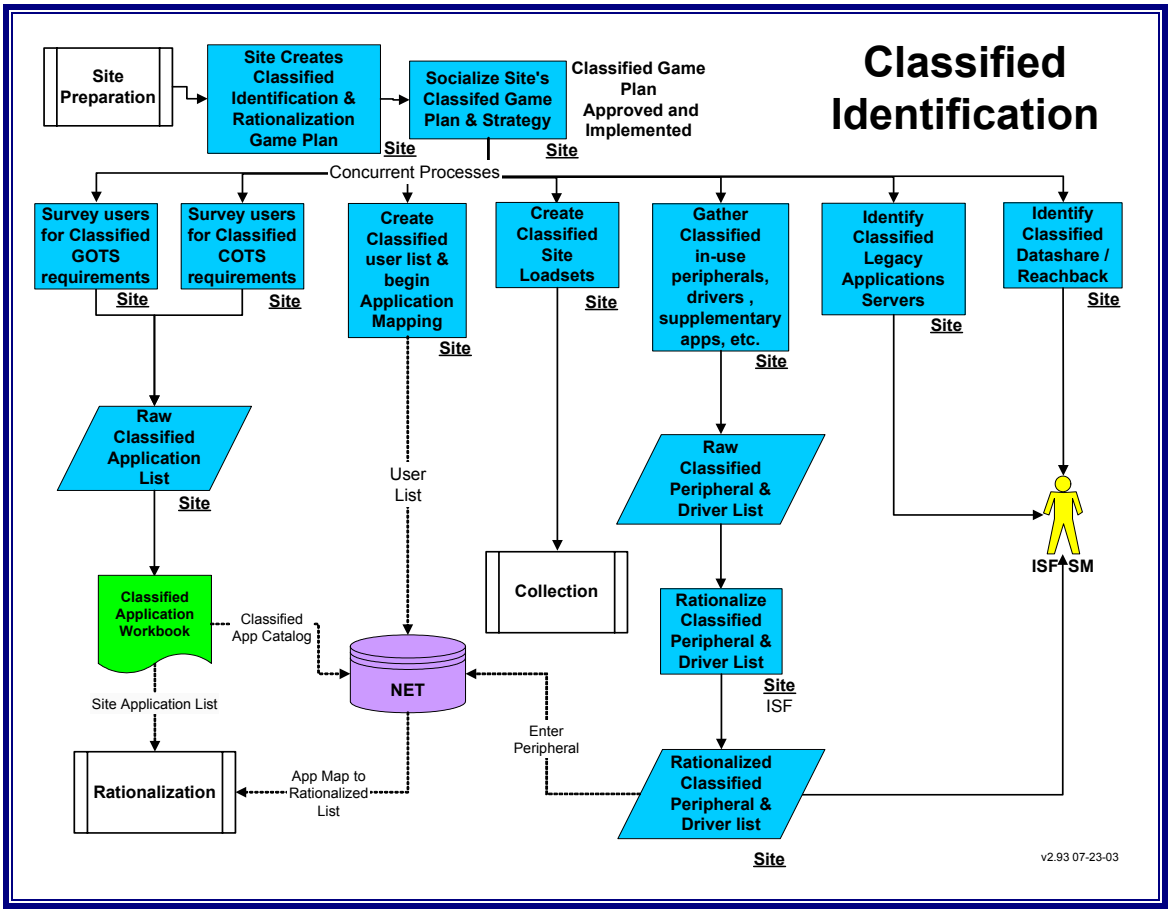


Figure F-4. Classified Identification

3.2.2 Classified Application Rationalization

Once again, the Classified Legacy Applications Rationalization process differs from the unclassified process in the use of the ISF Tools Database. Once the applications have been identified in the Raw Classified Applications List, the Command/Site applies the rationalization steps as depicted in the unclassified processes of this guide. See Figure F-5 for details of the classified application rationalization process.

Classified Legacy Applications Rationalized List Template

The following information only pertains to sites with legacy applications running in the classified environment. Sites should use the ISF Tools Database (see section above) to identify their legacy applications running in the unclassified environment and create their Rationalized Lists for those applications.

Sites with legacy applications running in the classified environment should use the Classified Legacy Applications Rationalized List Template <downloads/ClassRatListTemplate.xls> [Version 1.1, Posted December 18, 2002] to identify those applications and build their classified Rationalized Lists. After the classified Rationalized List has been completed, it must be taken to the site's Information Systems Security Manager/Information Systems Security Officer (ISSM/ISSO) to determine whether the list itself is classified.

- If the classified rationalized list is deemed unclassified, it should be sent via unclassified e-mail to EDS' classified applications Product Delivery Analyst (PDA).
- If the classified rationalized list is deemed classified, it should be sent via classified e-mail or another approved delivery method to EDS' classified applications product delivery analyst (PDA).
- Information that is too big to send over classified email can be sent by registered mail following the classified guidelines of Chapter 10 in the ISF Security Policy Manual located on the Knowledge Base website.
- The EDS PDA is Paul Halpin, and he can be reached at the following email paul.halpin@nmci-isf.com for unclassified information and paul.halpin@nmci.navy.smil.mil for classified information.

EDS will assign Classified Request for Service (CRFS) numbers to the classified legacy applications listed. This information will be put in a Site Classified Applications Workbook and sent to the site in the same manner it was sent to EDS (via a classified method/e-mail or unclassified e-mail). The site can then use the appropriate CRFS number when completing the CRFS document for each classified legacy application. For more information on completing the CRFS document and submitting classified legacy applications, please see the section below entitled Legacy Application Certification/Validation. <transition.htm>

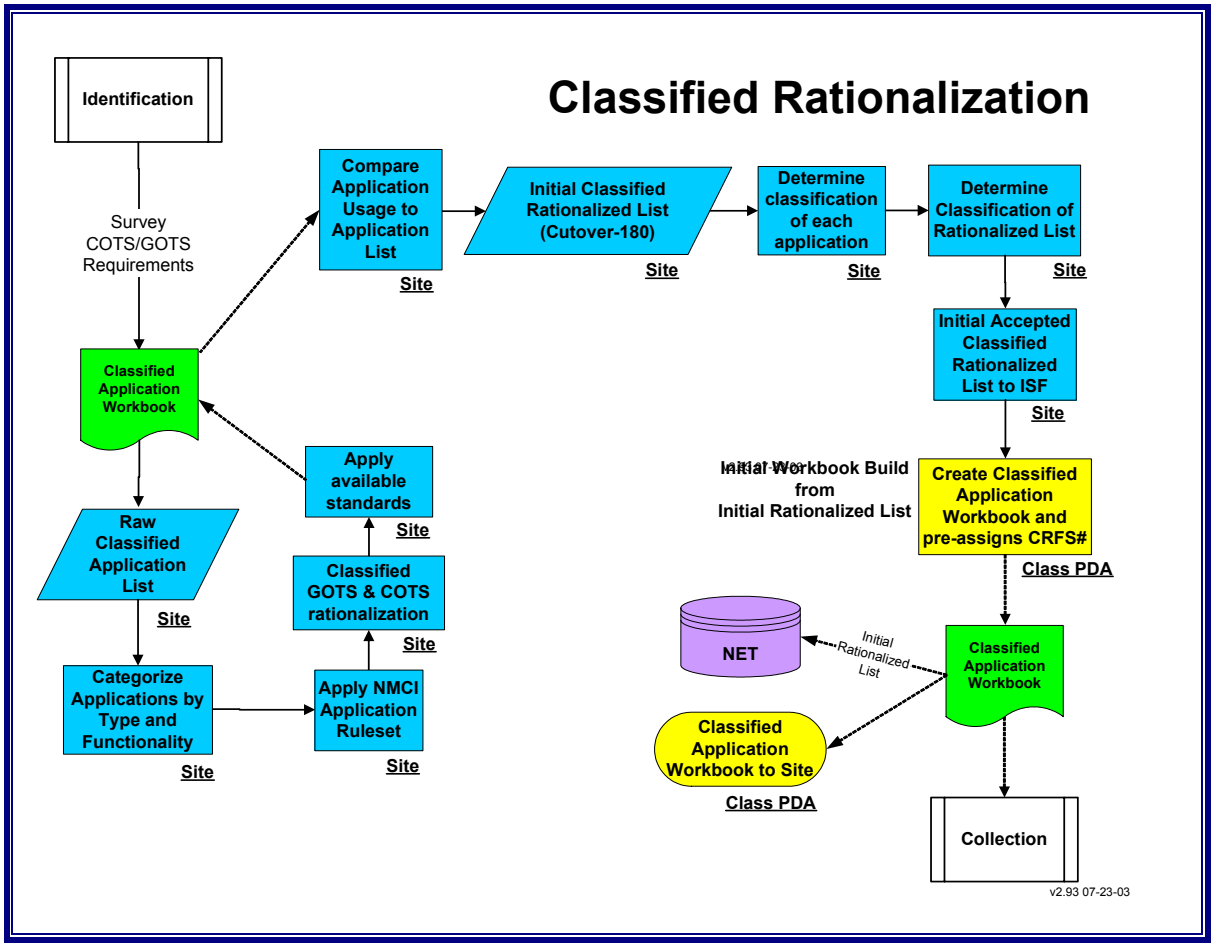


Figure F-5. Classified Rationalization

3.2.2.1 Initial Classified Rationalized List

Those applications from the Raw Classified Applications List that remain after the rationalization process are listed in the Initial Classified Rationalized List.

Instead of using the ISF Tools Database, the site creates the Initial Classified Rationalized List using the template found in Enclosure 2 or downloaded from the EDS NMCI website at http://www.nmci-isf.com/transition.htm.

3.2.2.2 Classified Applications Workbook

3.2.2.2.1 Classified Product Delivery Analyst (CPDA)

There is only one CPDA for all classified applications and he/she is located at the Classified AIT Lab in San Diego, California. The CPDA provides process support on the submission of classified Legacy Applications, training, Classified Workbook support, data analysis and progress reporting.

In addition, the CPDA will work with on-site SSE Teams to ensure readiness of applications and associated documentation prior to and during testing. The CPDA also works with all members of the Legacy Applications Transition team to ensure that proper documentation standards are kept. The CPDA

interfaces with government and EDS personnel, including (but not limited to): STEM, PMO, NADTF, DMT, PEO-IT, PDM, SSE Team members, SM, Customer Technical Representative (CTR), LAPOC, AIT, EAGLE and IA Teams. CPDA responsibilities include:

- Review, analyze and provide documentation on LADRA readiness and Rationalized List status for the Pre-AOR Review.
- Create reports for EDS Legacy Applications management.
- Identify applications submitted that already have a documented NMCI solution (Certification by Association (CBA)).
- Provide process guidance and Classified Workbook training to EDS and Navy personnel on the submission of Classified Legacy Applications and peripherals.
- Investigate media and documentation issues (CRFS, etc.).
- Participate in recurring site status meetings to provide support and problem resolution.
- Conduct Readiness Review (RR) and Post Cutover Assessment (PCA) to ensure readiness of site applications and final status.

The CPDA will continue to work with a site after Cutover is complete to make sure that the transition is complete and went well.

3.2.2.2 Classified Applications Workbook

The EDS CPDA uses a Microsoft Excel spreadsheet to create the Site Classified Applications Workbook to organize information about the sites' legacy applications as they undergo certification. The Workbooks are created and maintained by the PDA. They initially create workbooks from a customer's Initial Classified Rationalized List of applications. As applications move through the certification and testing processes, the workbook is updated by the CPDA to show status. These updates vary in frequency, but they usually occur weekly and then daily as the site approaches Cutover.

The preferred method for Command/Sites to monitor the progress of their submitted applications is to work the workbook with the CPDA. This interaction usually takes the form of Site-Specific Workbook Reconciliation meetings. These are phone conferences between the CPDA, site LAPOC, the PMO, STEM, and other interested parties. The goal of these conferences is to keep the workbook current so that it portrays a clear picture of a site's applications with respect to certification. The creation of a workbook usually happens after a Command/Site completes their Initial Classified Rationalized List at Cutover minus 180. The Rationalized List and workbooks are considered classified documents, as they may contain classified information.

As applications are entered into the workbook, they are pre-assigned a Classified Request for Service (CRFS) number. This occurs before a CRFS is actually submitted. As the Classified Application Workbook is done manually, CRFS numbers are assigned manually. Then, once the Command/Site submits the CRFS, the pre-assigned CRFS number becomes permanent.

The EDS PDA is responsible for keeping the Command/Site informed on all progress associated with the certification and testing effort. This progress status communication may be accomplished in any number of ways, such as: phone conversations, customer request, designated workbook meetings, etc. The EDS

AIT Classified Legacy Applications Lead will utilize the Secret Internet Protocol Router Network (SIPRNET) to pass along more detailed information when required.

3.3 Classified Collection

The Classified Collection process is a Government responsibility. Secure handling procedures, personnel security clearances; custody, and storage are all factors that have to be addressed during this process. Figure F-6 depicts the steps of this process.

After the Classified Application Workbook is formulated by the CPDA, the legacy application media and supporting documentation must be collected for submission to the EDS SM for NMCI Certification.

Classified Legacy Applications require the following:

- For Official Use Only (FOUO) CRFS (available at http://www.nmci-isf.com/transition.htm)
- Media and License Verification
- Installation Instructions and Test Scripts
- Network Diagram (desktop-to-server connectivity)
- Test Plan
- Risk Mitigation Engineering Review Questionnaire (RMERQ) (available at http://www.nmci-isf.com/transition.htm - Engineer)
- POC information on Technicians, Programmers or Systems Administrators

Sites do not have to provide proof of all licenses needed for all of the users of an application. However, proof of licensing is required for the copy of the application that is being submitted for NMCI Certification Testing. If a license is not available, proof must be obtained and submitted.

NOTE: In most cases the use of legacy applications without an approved license is a violation of applicable copyright laws and is expressly prohibited. EDS will test and make recommendations on all legacy application software submitted to them in an effort to facilitate the efficient movement of seats into the NMCI environment. However, the sole responsibility for ensuring proper maintenance and distribution of licensing for transitioning legacy applications rests with the individual Command/Site/Echelon II/CDA transitioning those applications.

If any prior Interim Authority to Operate (IATO) or DoD Information Technology Security Certification and Accreditation Process (DITSCAP) documentation exists for a legacy application being submitted, it should be collected and stored by the Command/Site for use in the Risk Mitigation Phase. The Application Mapping must be completed and turned over to EDS Site Manager. Final Application Mapping is due with the Final Classified Rationalized List at Cutover -120. Navy Applications Database Task Force (NADTF) will use the Application mapping as they perform enterprise rationalization and standardization.

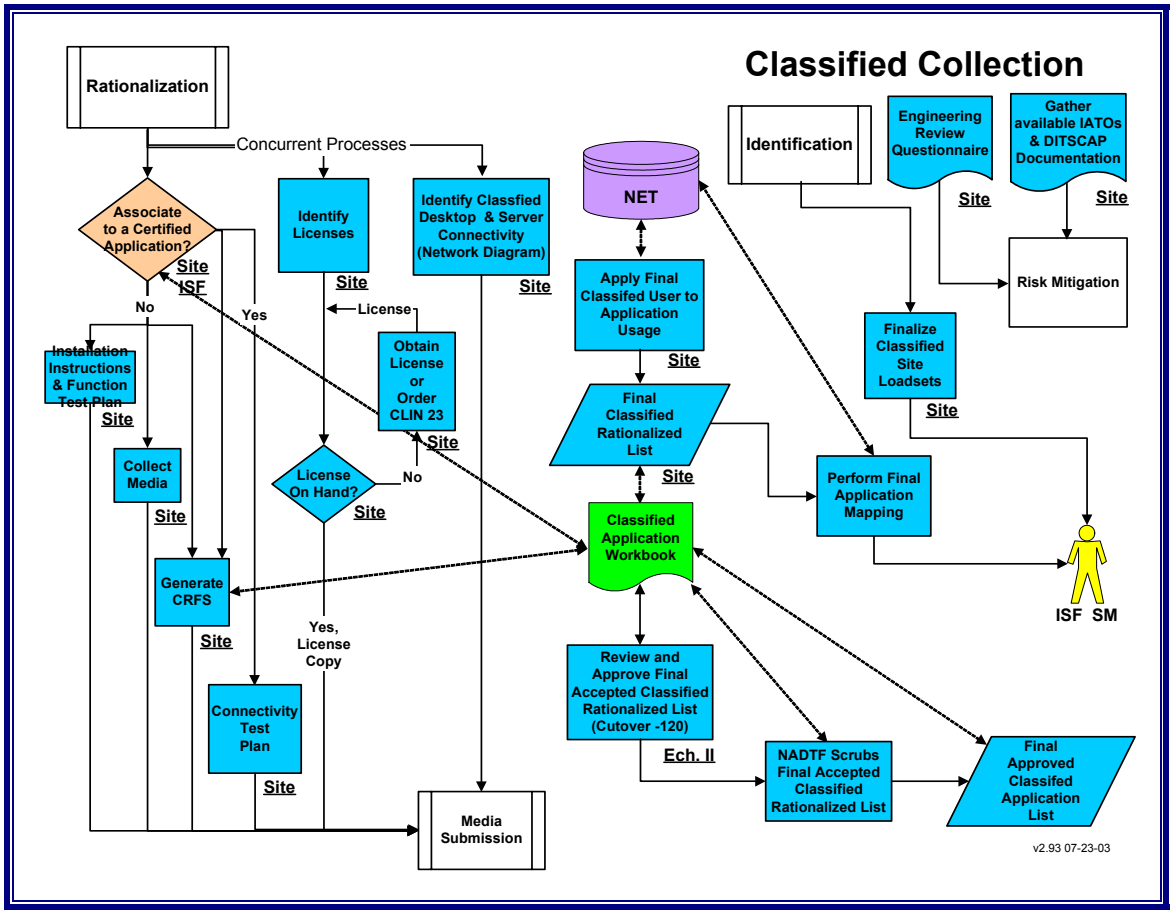


Figure F-6. Classified Collection

3.4 Classified Media Submission

It has been determined that the majority of applications residing on the SIPRNET are Unclassified except when populated with classified data. If the site has an application that itself is classified even without data, the Command/Site will complete the FOUO CRFS form, mark it (classification) appropriately, prepare the media, and submit both to the EDS SM.

Classified Legacy Applications Media Submission (Figure F-7) is different from the Unclassified Media Submission in the adherence to appropriate security procedures for handling and storage of classified information. The Command/Site Information System Security Manager/Officer (ISSM/O) will be responsible for securing all classified software and documents. The Command/Site ISSM/O will review all completed RMERQs and Network Diagrams provided to the EDS SM and/or the EDS Site Solutions Engineering (SSE) Team Lead to determine their classification due to the level of detail they contain.

If they become classified material, the appropriate handling procedures are invoked per the level of classification. RMERQs and Network Diagrams are required for on-site or off-site testing and certifications. All applications will require the RMERQ form completed prior to the Risk Mitigation Phase. The EDS will not have secure storage facilities on-site; the Site ISSM/O is required to provide secure storage and EDS access.

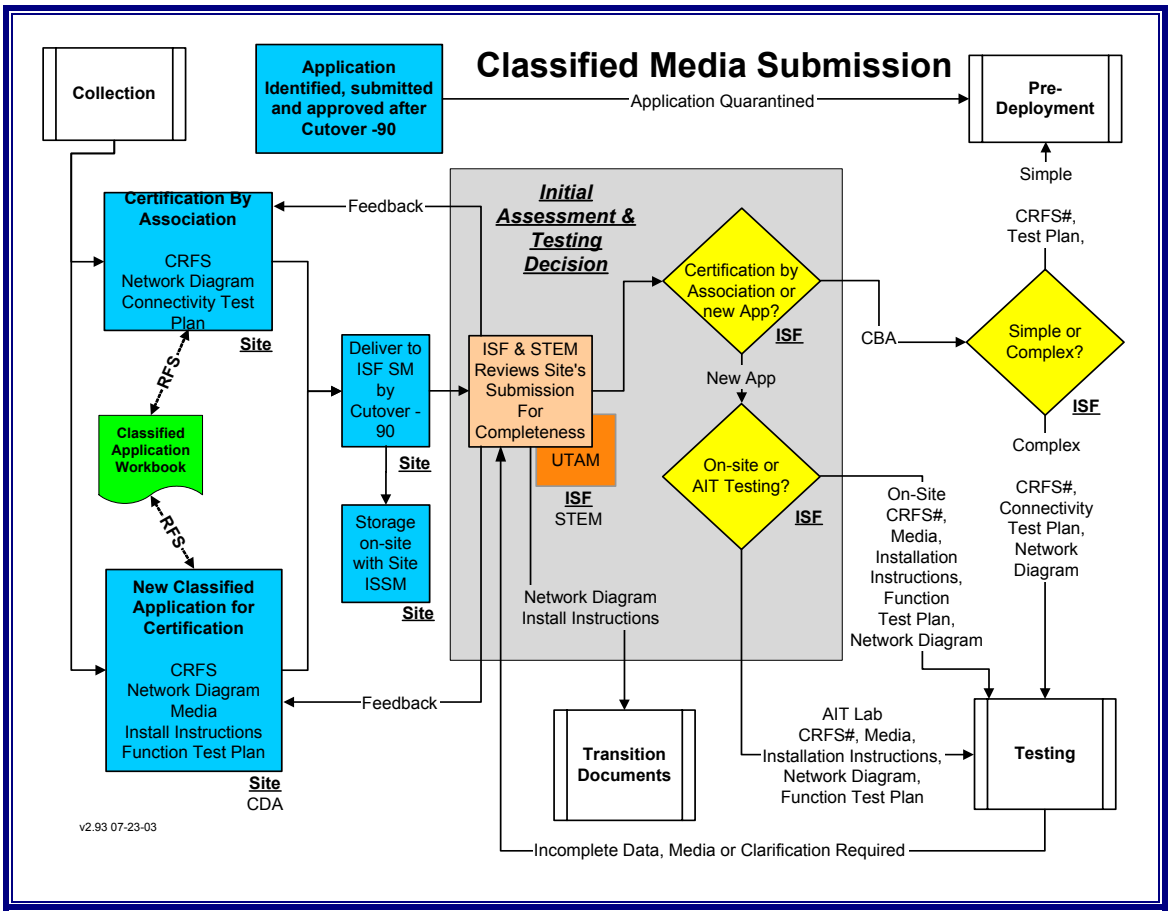


Figure F-7. Classified Media Submission

After an application's media and support materials are collected, they must be submitted to the on-site EDS SM to begin the NMCI Certification process. If the EDS SM has not arrived on site, the Command will hold all materials until the EDS SM arrives. Tracking at the EDS level will commence upon receipt of the material. Each application will be assigned a tracking number ('CRFS Number') by the PDA.

The EDS SM will turn the submission over to the EDS SSE Team Lead. The EDS and STEM teams will perform an initial assessment of the submission in the Completeness Review. If any parts of the required submission are missing or incomplete, the STEM and EDS will work with the Command/Site to provide them. If the submission passes the completeness review, the EDS then determines which testing activity the application will be sent to for processing.

In most cases the scheduling of applications for certification/testing will be done by the on-site SSE Team. Further, the SSE Team Lead will determine whether Testing will occur on-site via the CPIAB and/or the Classified NMCI Test Seat in the Local Deployment Solutions Development and Testing (LDSD&T), or sent for Certification to the Classified Application Integration & Testing (AIT) Lab located at the San Diego Network Operations Center (NOC).

3.4.1 Submission Deadlines

All applications are due to the EDS SM NLT Cutover minus 90. Any applications submitted late are subject to the Late Identification and Submission Process. (See Appendix E.)

3.5 Testing

The Government and the EDS share joint responsibility in this process, but the EDS conducts most of the work.

Testing is broken down into two separate areas, each performing a unique and specific function necessary in the preparation of a transitioning application and comprising the core transition methodologies capable of covering a wide range of software and application implementation strategies. These two separate areas are the Lab Testing and On-Site Testing.

Once the completeness review is done, the EDS SM and STEM make a determination on the best method to process an application for inclusion in NMCI. Four testing approaches are available:

- Classified San Diego Packaging and Certification Lab (CAIT)
- CAL
- PIAB
- LDSD&T

The PIAB and LDSD&T are done on site and the other two (CAL and the Classified San Diego Packaging and Certification Lab) are accomplished off site. For all practical purposes the methods used in the processing of classified applications are identical to those used in the unclassified process, the only differences being the manual tracking through the Classified Workbook and the special security requirements for storage, handling and personnel clearances.

Because the classified environment is connected to the SIPRNET, all information, media, and data collected during testing must be handled in a secure manner.

3.6 Classified Application Transition Documentation

The Transition Documentation process is an EDS responsibility. The process is the same for classified and unclassified applications, with the obvious exception of the storage and handling of the documents. Below is a list of Security Documents for reference.

Security Documents

- DOD 5220.22S COMSEC Supplement for Safeguarding Classified Information
- DOD 5220.22M National Industrial Security Program Operating Manual
- SECNAVINST 5510.30A Department of the Navy Personnel Security Program Regulation
- SECNAVINST 5510.36 Department of the Navy Information Security Program Regulation
- Conducting NMCI Classified Meetings
- How To Transmit And Transport Classified Materials

- Defense Courier Service Regulation
- Guidance For Handling Controlled Unclassified Information (CUI), Sensitive And Classified Information For Navy/Marine Corps Intranet (NMCI)
- Safeguarding Classified and Controlled Unclassified Information
- SF 312 Non Disclosure Agreement
- IA PUB 5239-26 Information Assurance Remanence Security Publication PIAB MANAGER Reference when removing PIAB from Classified Enclave.
- SIPRNET Security Classification Guide

In the Testing processes there are two distinct methods available for preparing an application for inclusion on an NMCI seat: Local Deployment, which is done at the site and involves preparing the application for manual distribution to the desktop and centralized distribution (Push via Novadigm Radia) which is accomplished at the Classified San Diego AIT Lab or the CAL. There are no significant differences in processing classified legacy applications via Local Deployment or Push, except where previously described in this appendix.

During the testing processes the application status is recorded and tracked in the Classified Workbook. The Classified PDA, AIT Lab personnel and SSE teams will record the status of the various steps in the process.

3.5.1 Local Deployment vs. Push

As indicated in the main guide the application will be Pushed or Local Deployed to the desktop. The methods, steps, procedures, and processes for deploying applications in the classified environment are the same as in the unclassified environment, with the exception of the special security considerations for classified applications.

NOTE: The EDS has the responsibility to determine the most effective way to deploy a Legacy Application, and they will route the Legacy Application to the appropriate testing location and method.

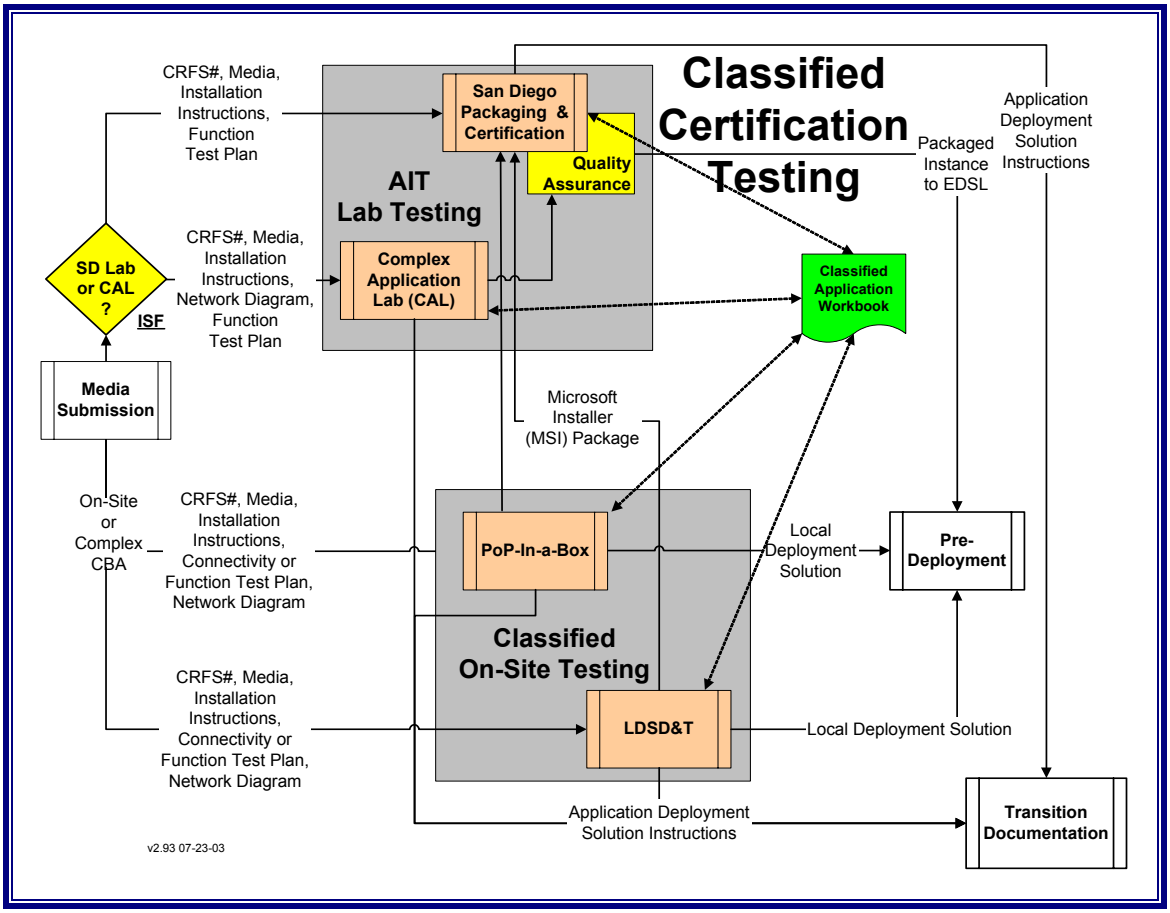


Figure F-8. Classified Certified Testing

3.5.2 San Diego Classified Packaging & Certification

Those applications selected for San Diego Packaging and Certification are sent to the San Diego Classified Application Integration and Testing (CAIT) Lab by the EDS with the help of the ISSM/O. Figure 9 depicts the Classified Packaging and Certification Lab processes. Applications go though a Packaging Audit by EDS personnel in the lab to verify that the packet is complete and that the media submitted is valid with no viruses. Any installation instructions are tested for completeness. The site is notified of problems with any submissions via SIPRNET by the EDS AIT Classified Legacy Applications Lead. With the exception of manual tracking through the Classified Workbook and the NMCI Certification Letters, which will be generated soft-copy and transmitted via E-mail or SIPRNET, all of the procedures in this process are the same as those depicted in Section 4.0 of the main guide.

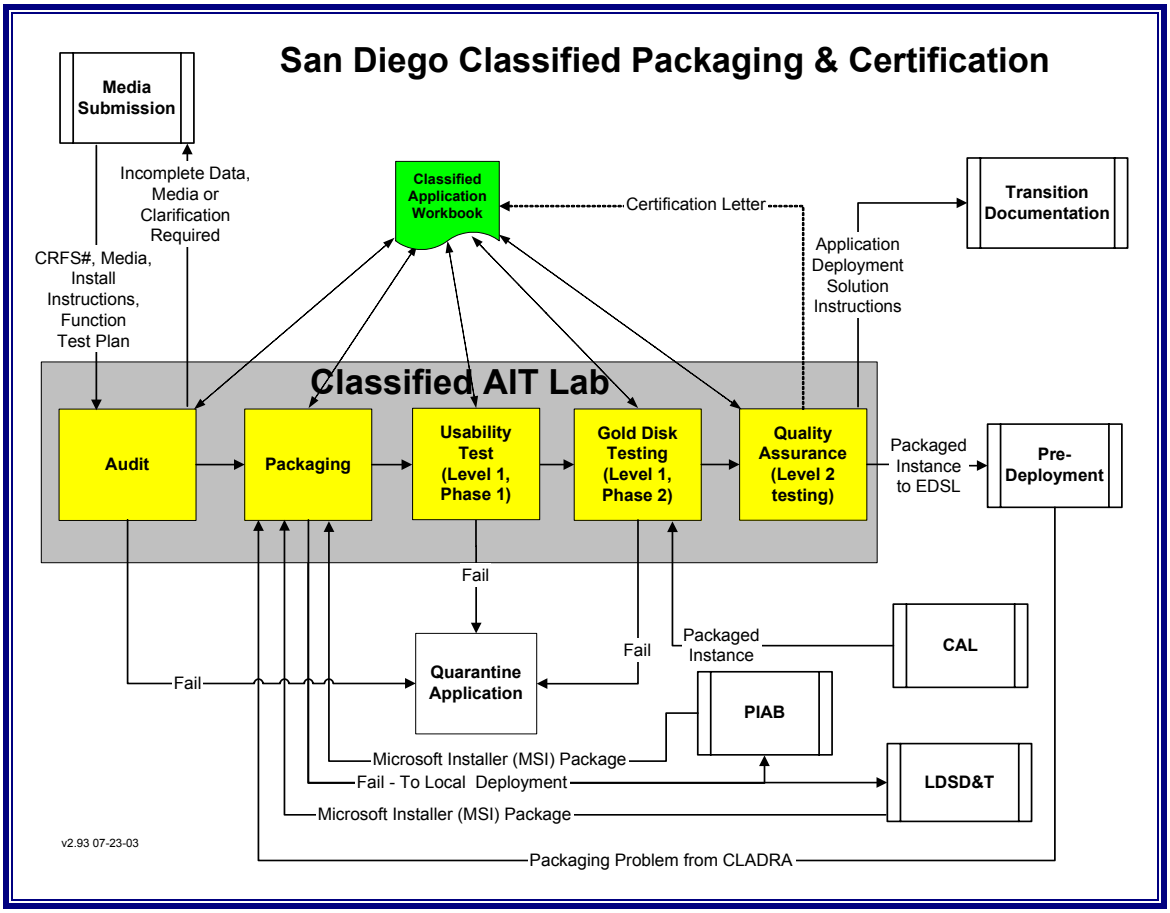


Figure F-9. San Diego Classified Packaging and Certification

3.5.3 Classified Complex Application Lab (CAL)

Figure F-10 depicts the CAL process. EDS uses the CAL to process CDA applications and to provide enterprise solutions. However, EDS may use the CAL to provide solutions for transitioning Classified Legacy Applications. The CAL operates in a secure environment within the Network Operations Center (NOC). Therefore both classified and unclassified media may be processed through the same equipment. With the exception of manual tracking through the Classified Workbook, SIPRNET, and special handling requirements, all of the procedures in this process are the same as those depicted in Section 4.0 of the main guide.

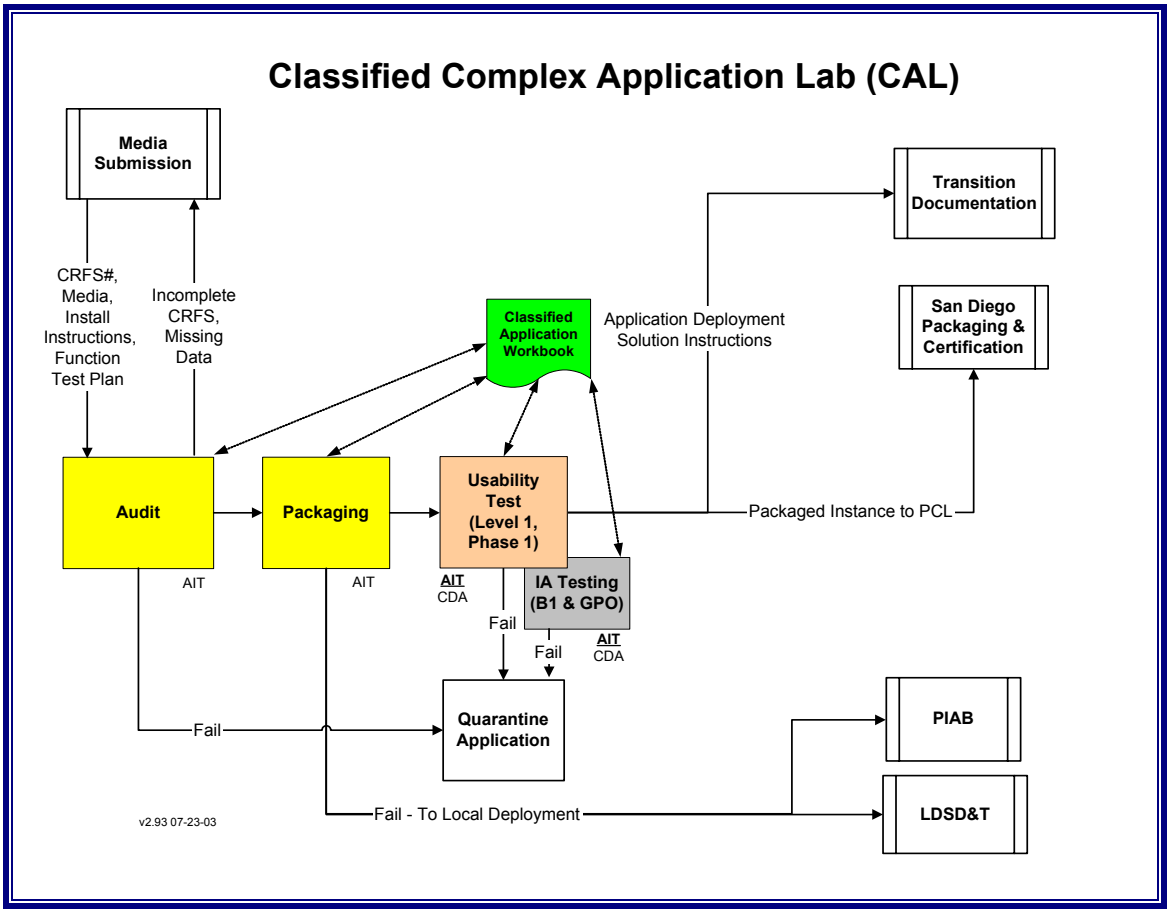


Figure F-10. Classified Complex Application Lab

3.5.4 On-Site Testing

Applications retained on-site for Local Testing are evaluated for their suitability for packaging and electronic push to the desktop. Applications selected for local packaging will proceed through Packaging steps by the EDS Site Solutions Engineering (SSE) team using the CPIAB, if available. Those selected for Local Deployment will be processed through the CPIAB or run through LDSD&T. There are no significant differences in processing classified legacy applications with regards to On-Site Testing, except where previously described in this appendix.

3.5.5 Classified PoP-In-A-Box (CPIAB)

The CPIAB is a separate suite of equipment from the unclassified PIAB. Classified applications may not be processed on an unclassified PIAB. Because there are so few CPIABs, a Command/Site may not receive the use of this tool and may have their applications processed through the Classified AIT Lab or CAL.

Processing classified applications through the CPIAB does not differ significantly from the unclassified processes, with the exception of the manual tracking of the Classified Workbook and the special security requirements for storage, handling and personnel clearances.

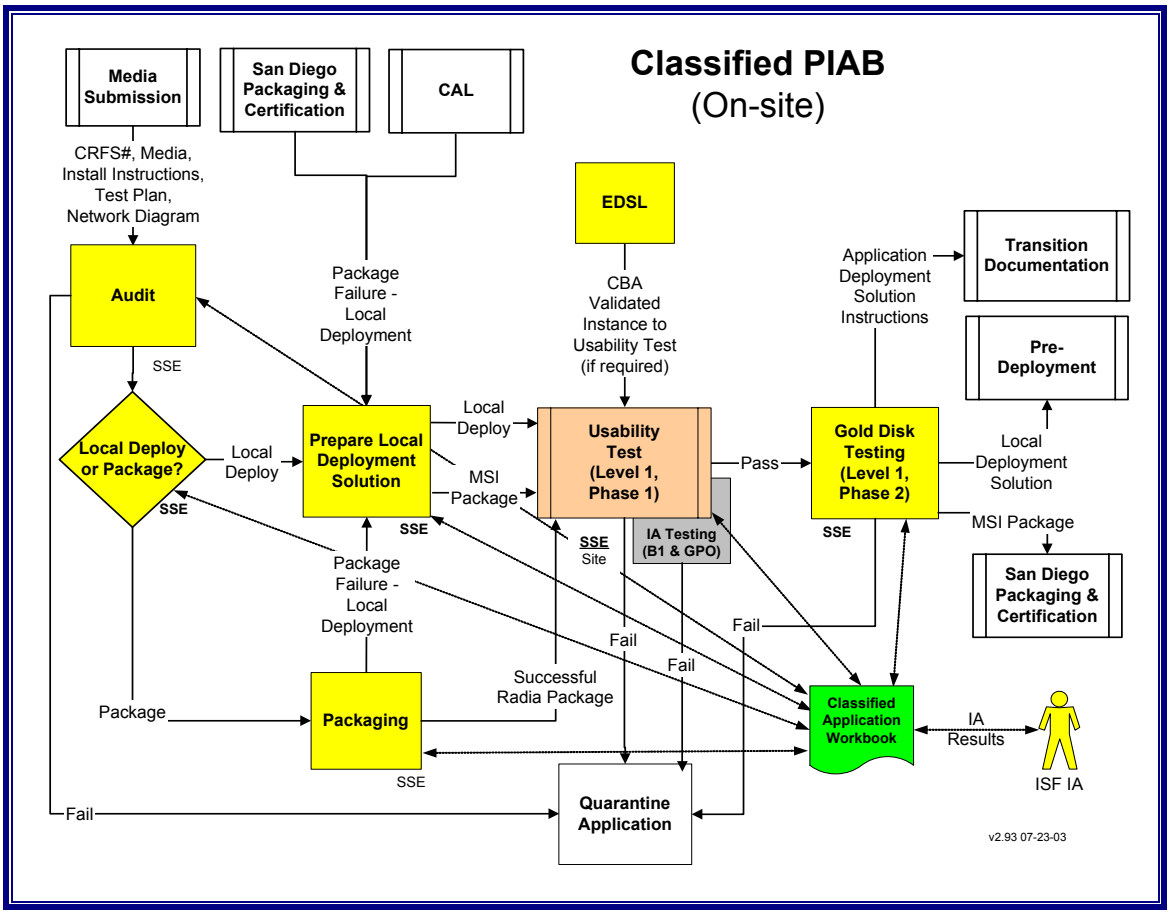


Figure F-11. Classified PoP-In-A-Box

3.5.6 Classified Local Deployment Solutions Development and Testing (CLDSD&T)

When a CPIAB is not available or deployed on-site, the SSE team will use an NMCI Test Seat to develop local deployment solutions for applications when the NMCI infrastructure is installed and active.

The Classified NMCI Test Seat will be used in the same manner as in the processing of unclassified applications, in the Rapid Certification Phase, to perform the Classified Usability Test. As indicated in Classified Site Preparation, where the requirements for processing of classified legacy applications were identified, application testing will be done on a Classified NMCI Test Seat that is housed in a secure environment.

The steps in the CLDSD&T do not differ significantly from those of the unclassified LDSD&T. The main differences are the use of the manual tracking of the Classified Workbook and the special security requirements for storage, handling and personnel clearances. The CLDSD&T process is depicted in Figure 12. During the CLDSD&T process, the testing and certification status is recorded and tracked in the Classified Workbook by the SSE team and the Classified PDA.

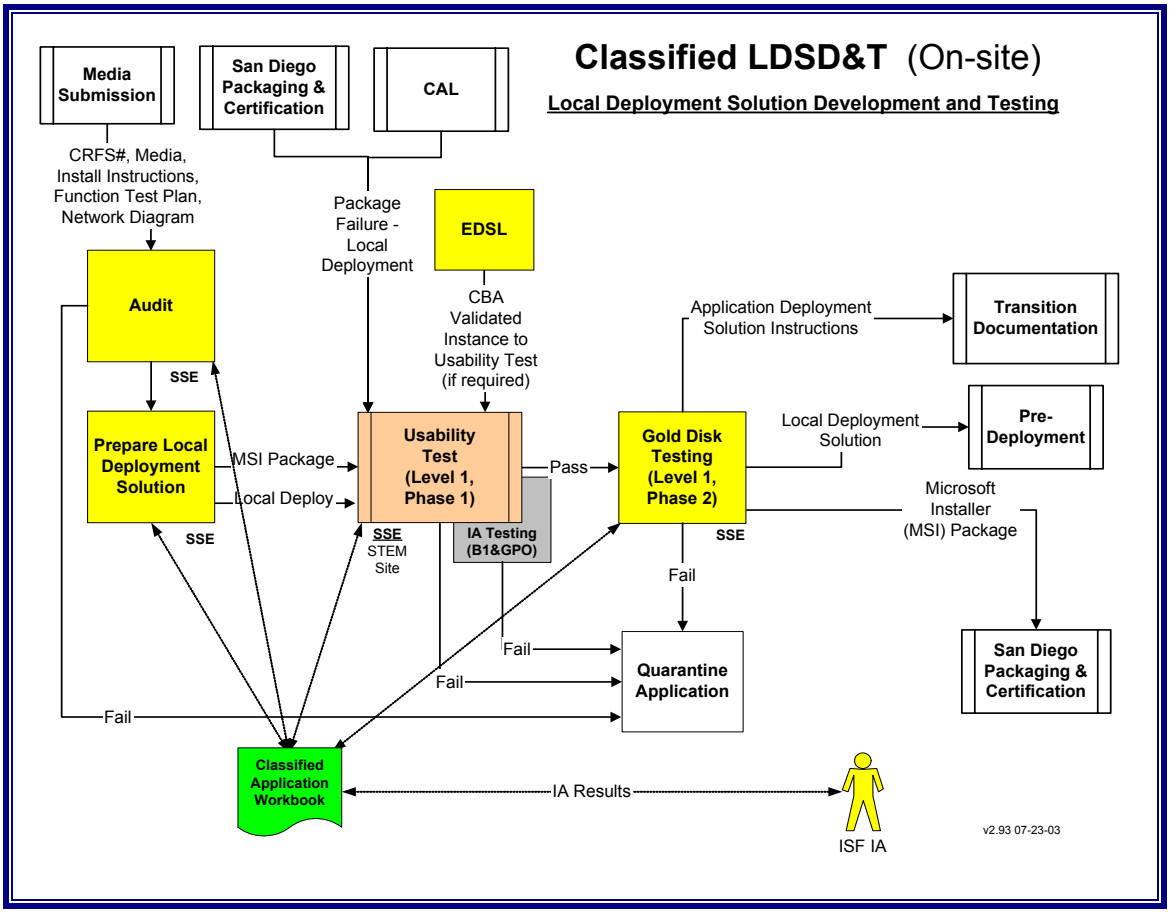


Figure F-12. Classified LDSD&T

3.6 Classified Application Transition Documentation

The Transition Documentation process is an EDS responsibility. The process is the same for classified and unclassified applications, with the obvious exception of the storage of the documents.

3.7 Information Assurance

The Classified NMCI Information Assurance (IA) process is similar to the Unclassified IA process except that there are no Boundary 2 (B2) and Boundary 3 (B3) requirements. Only Enterprise Boundary 1 (B1) and Boundary 4 (B4 or Group Policy Object (GPO)) are utilized in the Classified NMCI architecture. The Risk Mitigation Phase remains the same for classified and unclassified legacy applications and is beyond the scope of this guide. All other components, policies and procedures remain the same as the Unclassified NMCI environment depicted in the Guide.

3.8 Classified Pre-Deployment

The Pre-Deployment process is primarily an EDS responsibility. The Classified Pre-Deployment Process is the same as the Unclassified Pre-Deployment process, except the Classified Workbook replaces the EDS Tools Database and the Certification Letters are generated manually. In this stage, the final

preparations are made before actual delivery of user seats. Figure F-13 shows the Classified Pre-Deployment process.

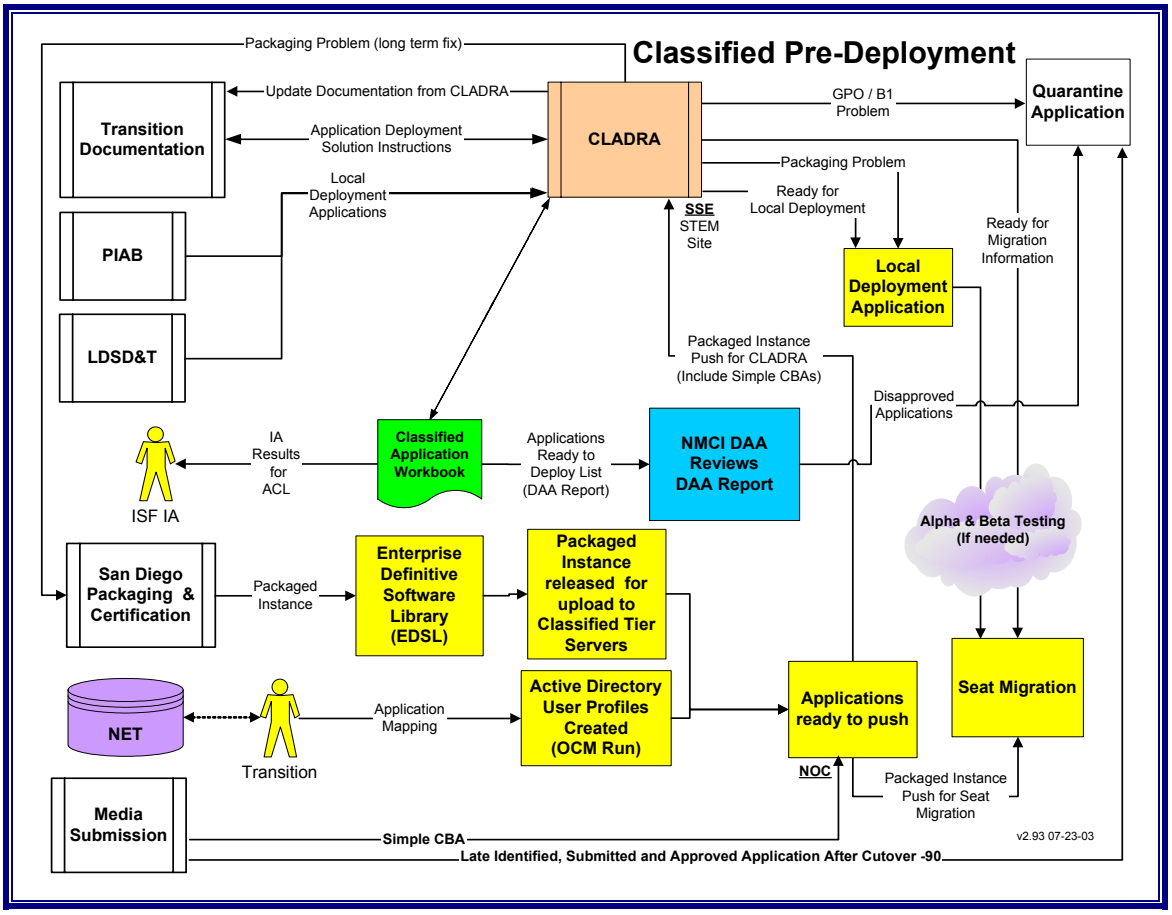


Figure F-13. Classified Pre-Deployment

3.8.1 Classified Legacy Application Deployment Readiness Activity (CLADRA)

The Pre-Deployment test is CLADRA. The CLADRA testing is a joint sub-process that is primarily an EDS responsibility.

CLADRA testing is conducted by the EDS in the live NMCI environment. The goal of CLADRA is to test 100% of the applications to be deployed to NMCI. In some instances, testing all applications may not be practical. The CLADRA test is designed to verify the transition solutions for the legacy applications. The steps of the CLADRA process do not differ significantly from the unclassified LADRA process. The use of the Classified Workbook to track status is the main difference.

All applications that successfully complete CLADRA testing are ready for Local Deploy or NOC Push to Seat Migration (Cutover).

Upon successful completion of CLADRA, the legacy applications are ready for the initial seat migration (Cutover).

3.8.2 Quarantine

Typically, a quarantined application is not allowed in the NMCI environment due to a violation of the NMCI Ruleset or testing. Applications that are quarantined remain operational in the Legacy environment. Failures can occur for many reasons, such as: non Win2K compliant, non Gold Disk interoperability, GPO/B1/B2 policy violations, late identification/submission, lack of Usability Testing support, and network connectivity errors. Some applications that violate the NMCI Ruleset will be Killed and removed from the Rationalized List. These Killed applications will not be utilized in NMCI and will not be quarantined. The guidelines for quarantined applications do not differ from the unclassified process.

4.0 —CONCLUSION

The transition of classified legacy applications is not significantly different from the processing of unclassified legacy applications. With the exception of special handling, security, and storage procedures, manual tracking via the Classified Workbook, most of the steps, procedures and processes remain the same as the unclassified processes depicted in the main portions of this guide.

APPENDIX G – TEMPLATES, SAMPLES, AND EXAMPLES

G1. Site Representation of Legacy Peripherals Template

Legacy Desktop Peripherals Requested for NMCI Transition								
Site Name:		Cutover Date:						
List Prepared By:		Preparation Date:						
Preparer's E-mail Address:		Preparer's Phone #:						
Manufacturer	Device Type	Device Name/ Model	If there is any bundled application associated with this device that has been added to your site's Legacy Application Rationalized List, list the application's RFS # and name here.	If there is a driver required that is not the default Windows 2000 driver, list it here.	User Name	Domain	Net ID	Comments
Example:								
Epson	*Printer*	*Stylus Color 850N*	*#123 Printer Pal*		*John Doe*	*CMDHQ*	*JDOE*	

Site Name: This is the official name of this site as it appears in the ISF Tools.

Cutover Date: This is the official scheduled Cutover date for this site.

List Prepared By: This is the name of the person designated by the site to create this list.

Preparation Date: This is the date that this list was created.

Preparer's E-mail Address: This is the email address of the person designated by the site to create the list.

Preparer's Phone #: This is the phone number of the person designated by the site to create the list.

Device Type: Examples: Printers, scanners, monitors

Device Name/Model: Enter the exact name and model number of the device.

If there is any bundled application associated with this device that has been added to your site's Legacy Application Rationalized List, list the application's RFS# and name here. An example would be photo-editing software that was bundled with a scanner. By doing this, RFS is created. If you don't know the RFS number, it can be found in the site's Legacy Application Rationalized List in the ISF Tools Database.

If there is a driver required that is not the default Windows 2000 driver, list it here. By default, the EDS will attempt to find the Windows 2000 driver for this peripheral. However, many devices have drivers that provide broader functionality than the default driver. List the file name of the driver here. The site will be required to provide this driver to the EDS if testing is required. There may be a CLIN 29service fee for any additional testing and reengineering. If the driver is not Windows 2000 compatible, impacts SLA performance or violates NMCI security policies it will not be allowed.

User Name: This is the user whose NMCI seat will connect to the device.

Domain: This is the user's new NMCI Domain.

Net ID: This is the user's new NMCI Net ID.

G2. Example Installation Instruction

The following is an example of an installation instruction that the ISF will use to install the release for testing.

Visio2000: Revised Network Installation Instructions (Network.wri) for
Visio 2000 Standard Edition
The information in this article applies to:
Microsoft Visio 2000 Standard Edition
This article was previously published under Q258467

SUMMARY
The Network.wri file that is included with Microsoft Visio 2000 Standard Edition contains incorrect instructions for how to perform a network installation.

This article contains the full text of the Network.wri file, with the corrections incorporated. Use the information in this article instead of the Network.wri file when you need to do either of the following:
Install Visio 2000 Standard Edition to a network drive for shared use.
-or-
Install Visio 2000 Standard Edition locally from a network drive.

MORE INFORMATION
Visio® 2000 Standard Edition
Network Installation Instructions
Copyright© 1991 - 1999 Visio Corporation. All rights reserved.
File version 6.0.0 Visio(R) 2000 Standard Edition US English version
Network Installation Instructions
This file contains information about setting up and running Visio 2000 on a network.
We recommend that you read this file and keep a printed copy with your Visio documentation. For other late-breaking information about installing and running
Visio 2000, see the README.WRI file. For a list of all the files copied to your hard drive if you install the complete version of Visio 2000, see the
FILELIST.WRI file.

CONTENTS

1. NETWORK LICENSING INFORMATION

To run Visio on a network that gives more than one person access to the product, you need to acquire additional licenses either by purchasing additional retail packages of Visio or by purchasing license packs.

A license pack, which authorizes one additional user, includes a product license, a serialized registration card, and a documentation order form.

2. OPERATING SYSTEM REQUIREMENTS FOR VISIO 2000

To use Visio 2000 Standard Edition, you must be running one of the following 32-bit Microsoft Windows operating systems:

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT 4.0 (Service Pack 3 or later is required)

Service Packs for Windows 95, Windows 98, and Windows NT operating systems can be obtained from Microsoft Corporation (www.microsoft.com).

NOTE: To install Visio 2000 on a workstation running Windows NT 4.0, the user installing the product must have Administrator privileges for that workstation.

NOTE: Installation Path Length Limitation: To ensure operation of the Visio 2000 Solutions the directory chosen for installation of Visio 2000 Standard Edition must have a path name of less than 55 characters in length.

3. NETWORK SETUP OVERVIEW

Setting up Visio on a network is a two-step process: First, you install Visio on the network server; second, you set up individual workstations so they can run Visio from the server or from each workstation's hard disk.

NOTE: Setting up Visio 2000 on a network server for shared use requires Windows NT 4.0 SP 3 or later. This procedure is not supported under Windows 95 or Windows 98.

For details about setting up Visio on a network so that multiple workstations can use a shared copy from the server, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE" below.

For details about setting up Visio files on a network server so that the program can be loaded onto the hard disks of individual workstations, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS" below.

4. PREPARING A WORKSTATION TO SET UP VISIO FOR SHARED USE

The Visio 2000 setup program is based on the Microsoft Installer (MSI) technology. MSI must be installed on the workstation you are using to set up Visio 2000 for shared use before starting the Visio 2000 setup program. If MSI is not installed on the workstation, or if you are in doubt, use the following procedure to install MSI:

1. Insert the Visio 2000 CD into your CD-ROM drive.
2. From the Start menu, choose Run.

3. Type d:\Install\bin\sp\MSI\WinNT\InstMSI, where d is the letter assigned to your CD-ROM drive.

After installing MSI, complete the following procedure to install Visio 2000.

5. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE

To install Visio 2000 on a network server for shared use:
You must have write access to the network server to install Visio on the server.

NOTE: Do not run the Setup.exe file located in the root directory of the Visio CD for this procedure. This file is for single-user installations only, and will not install Visio correctly for shared use.

1. From a workstation running Windows NT 4.0, log on to the network and connect to the drive where you want to install the Visio program.
2. Insert the Visio 2000 CD into your CD-ROM drive.
3. From the Start menu, choose Run.
4. Type d:\Install\Setup /a where d is the letter assigned to your CD-ROM drive.
5. Setup prompts you for the location of your Visio installation.
6. Type e:\visio, where e is the letter assigned to the network server and Visio is the directory on the server where the Visio program files will reside.
7. Follow the instructions on your screen.
8. Setup /a installs the Visio program files and creates the following subdirectory: Visio\Bin, for Visio product files.

To set up a workstation to run Visio from a network server:

1. On the workstation, from the Start menu, choose Run.
2. Type e:\Visio\setup, where e is the drive letter and \Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.

The workstation setup does the following:

- Installs or updates any Windows system and shared files required by Visio.
- Adds Visio 2000 to the Start Menu.

6. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS

You can place Visio 2000 files on a network server by following the steps in the preceding section, "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE." Then, users can connect to the directory and run the Setup program to install Visio on their workstations.

To install Visio 2000 from a network server to a workstation

1. On the workstation, from the Start menu, choose Run.
2. Type f:\visio\setup where f is the drive letter and Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.
4. When Setup prompts you for an installation location, type c:\program files\Visio, where c is the letter assigned to the workstation hard drive and \program files\Visio is the directory on your workstation where the Visio program will reside.

7. DEFINING DEFAULT FILE PATHS FOR VISIO FILES

Users can define default file paths for Visio drawings, templates, add-ons, and filters. To specify these custom paths, choose Options... from the Visio Tools menu, and then click the File Paths tab. File paths defined here are written into the user's registry under the HKEY_LOCAL_MACHINE\Software\Visio\Visio 2000 key. Click the Help button on the File Paths tab for more information.

8. OPENING VISIO FILES ON A NETWORK

Working with and opening Visio files on a network is essentially the same as on an individual workstation. On the network, however, you can make a drawing available to other users and allow them to make changes to the file. You can also protect the file from changes.

* Keep the following issues in mind when using Visio on a network:
You can share stencil files so that multiple users can access them at once. However, when you share stencil files, it is important that users not open them in read/write mode. (When a Visio drawing file is opened in read/write mode, no other network user can access the file.)

By default, the read-only attribute is set for stencil files to prevent users from opening them in read/write mode. You can also set the network Visio directory to read-only to prevent users from opening the files in read/write mode.

9. USING FILTERS WITH VISIO IN SHARED WINDOWS ENVIRONMENTS

If you are using Visio 2000 in a shared Windows environment in which system files are write-protected, Visio 2000 cannot store custom filter settings. You will need to make changes to any filter defaults each time you use that filter – changes will not be retained from one use to the next.

Visio 2000 Standard Edition

END of Network Installation Instructions

G3. Example for Installation Instruction: Defense Information Infrastructure/Common Operating Environment

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Installation Procedures (IP) for <name and version of software/segment>

<Document Version (if applicable)>

<Date>

Prepared for:

Defense Information Systems Agency

Table of Contents

<< GENERATE THE TABLE OF CONTENTS HERE >>

To generate the Table of Contents:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Contents* tab
3. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
4. Click on "OK" to generate the Table of Contents

List of Tables

<< GENERATE THE LIST OF TABLES HERE >> .....

To generate the List of Tables:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Figures* tab
3. Highlight *Table* in the Caption Label window
4. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
5. Click on "OK" to generate the List of Tables

List of Figures

<< GENERATE THE LIST OF FIGURES >>

To generate the List of Figures:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Figures* tab
3. Highlight *Figure* in the Caption Label window
4. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
5. Click on "OK" to generate the List of Figures

Notes on Using the Template

1. Refer to Section 3.1 and 3.2 of the *DII COE Developer Documentation Requirements* for format requirements and guidelines for using the templates.
2. This template has been formatted for a small document (12 pages or less). Section headings are left adjusted (refer to Section 3.1.6 of the *DII COE Developer Documentation Requirements*) and are not required to begin on a new odd page.

1. SCOPE

This section shall be divided into the following paragraphs.

1.1 IDENTIFICATION

This paragraph shall contain a full identification of the system and the software. It must provide the name(s), title(s), abbreviation(s), version number(s), and the release number(s). Identification must include the operating system platform(s) to which this document applies.

1.2 System Overview

This paragraph shall provide a brief description of the general nature, purpose, and function of the system/software. Provide references to additional information sources. Include documentation that may assist the user when problems are encountered. Identify each document-by-document number, title, version/revision, date, and source. Provide a point of contact to be used for reporting problems. Include facilities or organizations equipped to help in the event problems are encountered during installation. Identify organizations with mailing address, telephone number, fax number, and Web page or Internet address, as available.

2. Referenced Documents

Provide a list of documents referenced in this document. List each document-by-document number, title, version/revision, and date. Identify the source for all documents not available through the Government.

3. System Environment

Describe the system environment necessary to perform the installation of the software in this section. Include system and software configuration information, identify dependencies and compatibility issues, and provide any procedures that must be performed prior to installing the software.

3.1 System Requirements

3.1.1 Hardware Requirements

Identify all system hardware resources required to perform the software installation by name, number, type, size, etc. Provide the RAM and hard disk space required by the software/segment. Provide other requirements for computers, memory, drives, and other devices or components, as applicable.

3.1.2 Operating System Requirements

Identify the operating system and related components required to perform the software installation by names, version numbers, and release numbers, as applicable.

3.1.3 Kernel Requirements
Identify the DII COE Kernel version required to perform the software installation by name, version number, and release number, as applicable.

3.2 System and Site Preparations
Describe the system and site preparations that need to be performed prior to installing the software. Provide procedures for setting up the hardware and software, as needed. Identify hardware/software dependencies and exceptions to configuration, as applicable.

3.2.1 System Configuration
List any software or hardware components that must be installed and configured prior to the installation of the software (e.g., Telecom, Distributed Computing Environment (DCE), etc.). This section may cover requirements for upgrading specific system software with version dependencies.

3.2.2 Operating System Preparation
Provide procedures or information, if any, needed to prepare the operating system. Provide specific system requirements prior to installation (e.g., security, system privileges).

3.2.3 Tape/Disk Preparation
Provide procedures or information needed to prepare the tape or disk drive and related media, as applicable. Identify the physical media containing the software. Describe the disk partitioning and library set-ups that may be required.

4. Installation Instructions
Provide the step-by-step procedure and instructions for installing, configuring, and initializing the system software or segment into the appropriate libraries using the COE approved guidelines for segment installation and verification.

4.1 Media Booting Procedure
Provide instructions for booting the media containing the software, as needed, with specific options when required for the installation.

4.2 Installation Procedures
Provide the step by step procedures for configuring and installing the software. Provide instructions on how to load or download the software or segment into specific libraries using the DII COE approved guidelines for segment installation and verification.

4.3 Installation of Upgrades
Provide the step by step procedures and instructions for upgrading already installed software with new versions or patches. Identify the loading or downloading sequence and options for the software or segment installation.

4.4 Installation Verification
Describe procedures or a method (such as a checklist) for determining if the software installation was successful. This section may also describe and provide instructions for any software verification routines or programs provided, if any.

4.5 Initializing the Software

Describe the steps to be performed at the completion of the software installation. Include the procedures required for the initialization of system and software program operations.

4.6 List of Changes and Enhancements

Provide a brief description of the changes, enhancements, and fixes (patches) incorporated into this version of the software. Reference the applicable SVD for a detailed list of the software changes.

4.7 Important Considerations

Provide any security, licensing, privacy, and/or safety precautions and instruction relevant to the software being installed. This section may also provide critical back up and archiving instruction.

5. Notes

Provide general information to assist in the understanding of this document. This section may include a list of acronyms and abbreviations, and a list of terms and definitions.

6. Documentation Improvements and Feedback

Comments and other feedback on this document should be directed to the DII COE Hotline:

Phone: 703-735-8681
Fax.: 703-735-3080
Email: HotlineC@ncr.disa.mil

A. Appendices

Appendices may be used to provide additional information published separately for convenience in document maintenance. The appendices shall be referenced in the main body of the document, where applicable.

G4. Sample Test Script

This is an example of test cases and procedures used by the ISF to test the proper installation and functionality of the software.

Generating SQL Scripts for SMS Views

The information in this article applies to:

- Microsoft Systems Management Server 1.1
- Microsoft Systems Management Server 1.2

This article was previously published under Q133253

Summary

SMSVIEW creates various views that can be used when querying the Systems Management Server SQL Database. The SQL Scripts used to create these views can be dumped using Microsoft SQL Enterprise Manager (in Microsoft SQL Server 6.0).

More Information

To generate the SQL scripts to create the SMS views:

1. Start SQL Enterprise Manager.
2. If the server where the Systems Management Server database resides is not already registered in SQL Enterprise Manager, register it as follows:
    1. Select Register Server from the Server menu.
    2. Provide the server name and valid logon information (by default, the valid logon is SA with no password and Standard Security).
    3. Choose Register.
3. In the Server Manager window, select the server you just registered (there may be a slight delay as a connection to this server is established).
4. Choose in the following order:

    1. The Server's name in the Server Manager window.
    2. Databases to get to the Systems Management Server database.
    3. The database that contains the Systems Management Server data.

    The name of the SMS database in the Server Manager window should be selected.

5. Select Generate SQL Scripts from the Object menu.
6. In the Generate SQL Scripts - <servername>\<database name> dialog box, choose All Views for Scripting Objects. This fills in the name of each view in the list box at the bottom right portion of the dialog box.
7. Ensure Object Creation and Object Drop are selected for Scripting Options.
8. If you prefer scripts for each view to be placed in a separate file, select Per Object in Scripting Options. Otherwise, select Single File.

9. Choose Preview (there is a short wait as the scripts are generated). Save the scripts as text files or choose Close to go back to the Generate SQL Scripts dialog box without saving the scripts.

The following displays the resulting output (in Systems Management Server 1.1, Build 682):

```
/****** Object:  View dbo.vDisk    Script Date: 7/5/95 4:30:43 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vDisk') and
sysstat & 0xf = 2)
drop view dbo.vDisk
GO
Create View vDisk as select dwMachineID , Disk_SPEC.__Disk_Full0 ,
Disk_COMM.Disk_Index0 , Disk_COMM.File_System0 ,
Disk_SPEC.Free_Storage__MByte_0 , Disk_SPEC.Sectors0 ,
Disk_SPEC.Serial_Number0 , Disk_SPEC.Storage_Size__MByte_0 ,
Disk_COMM.Storage_Type0 , Disk_SPEC.Storage_Used__MByte_0 ,
Disk_SPEC.Volume_Name0 from  MachineDataTable  ,Disk_COMM   , Disk_SPEC
where Disk_COMM.datakey =*  CommonKey and Disk_SPEC.datakey =* SpecificKey
and ArchitectureKey = 5 and GroupKey = 8
GO
/****** Object:  View dbo.vEnvironment    Script Date: 7/5/95 4:30:43 AM
******/
if exists (select * from sysobjects where id =
object_id('dbo.vEnvironment')
and sysstat & 0xf = 2)
drop view dbo.vEnvironment
GO
Create View vEnvironment as select dwMachineID ,
Environment_SPEC.Environment_String0 , Environment_SPEC.Value0 from
MachineDataTable  ,Environment_COMM   , Environment_SPEC where
Environment_COMM.datakey =*  CommonKey and Environment_SPEC.datakey =*
SpecificKey and ArchitectureKey = 5 and GroupKey = 12
GO
/****** Object:  View dbo.vGroupNames    Script Date: 7/5/95 4:30:44 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vGroupNames')
and sysstat & 0xf = 2)
drop view dbo.vGroupNames
GO
Create View vGroupNames as select  GM.GroupName   FROM ArchitectureMap AM,
GroupMap GM  WHERE  GM.ArchitectureKey = AM.ArchitectureKey AND
((AM.Mode=0))
GO
/****** Object:  View dbo.vIdentification    Script Date: 7/5/95 4:30:44 AM
******/
if exists (select * from sysobjects where id =
object_id('dbo.vIdentification') and sysstat & 0xf = 2)
```

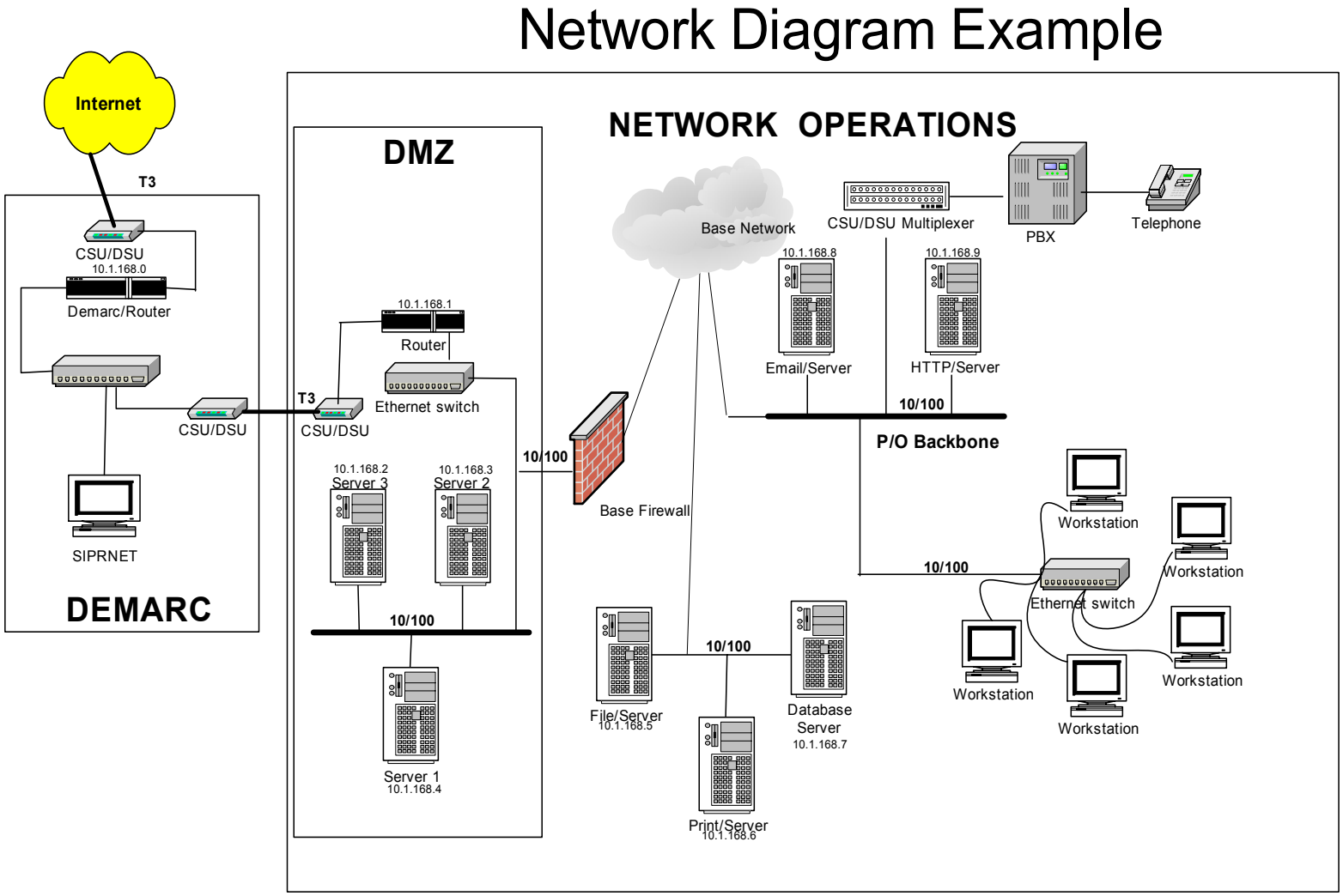
```
drop view dbo.vIdentification
GO
Create View vIdentification as select dwMachineID ,
Identification_SPEC.Domain0 , Identification_SPEC.LogOn_Name0 ,
Identification_SPEC.Name0 , Identification_SPEC.NetCardID0 ,
Identification_SPEC.Site0 , Identification_SPEC.SMSID0 ,
Identification_SPEC.SMSLocation0 , Identification_SPEC.SystemRole0 ,
Identification_SPEC.SystemType0 from  MachineDataTable
,Identification_COMM
, Identification_SPEC where Identification_COMM.datakey =*  CommonKey and
Identification_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 1
GO
/****** Object:  View dbo.vMouse    Script Date: 7/5/95 4:30:44 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vMouse') and
sysstat & 0xf = 2)
drop view dbo.vMouse
GO
Create View vMouse as select dwMachineID , Mouse_COMM.Hardware_Installed0 ,
Mouse_COMM.Language0 , Mouse_COMM.Manufacturer0 ,
Mouse_COMM.Mouse_Hardware_Type0 , Mouse_COMM.Number_of_Buttons0 from
MachineDataTable  ,Mouse_COMM   , Mouse_SPEC where Mouse_COMM.datakey =*
CommonKey and Mouse_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 4
GO
/****** Object:  View dbo.vNetcard    Script Date: 7/5/95 4:30:45 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vNetcard')
and
sysstat & 0xf = 2) drop view dbo.vNetcard
GO
Create View vNetcard as select dwMachineID , Netcard_SPEC.IRQ0 ,
Netcard_COMM.Manufacturer0 , Netcard_SPEC.Port_Address0 from
MachineDataTable  ,Netcard_COMM   , Netcard_SPEC where Netcard_COMM.datakey
=*  CommonKey and Netcard_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 11
GO
/****** Object:  View dbo.vNetwork    Script Date: 7/5/95 4:30:45 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vNetwork')
and
sysstat & 0xf = 2) drop view dbo.vNetwork
GO
Create View vNetwork as select dwMachineID , Network_COMM.Default_Gateway0
Network_SPEC.IP_Address0 , Network_SPEC.IPX_Address0 ,
Network_COMM.LogOn_Name0 , Network_COMM.Major_Version0 ,
```

```
Network_COMM.Minor_Version0 , Network_SPEC.Network_Active0 ,
Network_COMM.Network_Type0 , Network_COMM.Subnet_Mask0 from
MachineDataTable  ,Network_COMM   , Network_SPEC where Network_COMM.datakey
=*  CommonKey and Network_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 10
GO
/****** Object:  View dbo.vOperating_System    Script Date: 7/5/95 4:30:45
AM ******/
if exists (select * from sysobjects where id =
object_id('dbo.vOperating_System') and sysstat & 0xf = 2)
drop view dbo.vOperating_System
GO
Create View vOperating_System as select dwMachineID ,
Operating_System_COMM.Build_Number0 , Operating_System_COMM.Build_Type0 ,
Operating_System_COMM.Country_Code0 ,
Operating_System_SPEC.Installation_Date0 ,
Operating_System_COMM.Language_ID0 ,
Operating_System_COMM.Operating_System_Name0 ,
Operating_System_COMM.Registered_Organization0 ,
Operating_System_SPEC.Registered_Owner0 ,
Operating_System_SPEC.System_Root0
, Operating_System_SPEC.System_Start_Options0 ,
Operating_System_COMM.Version0 from  MachineDataTable
,Operating_System_COMM   , Operating_System_SPEC where
Operating_System_COMM.datakey =*  CommonKey and
Operating_System_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 7
GO
/****** Object:  View dbo.vPC_Memory    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vPC_Memory')
and sysstat & 0xf = 2)
drop view dbo.vPC_Memory
GO
Create View vPC_Memory as select dwMachineID ,
PC_Memory_SPEC.Page_File_Name0 , PC_Memory_SPEC.Page_File_Size__MByte_0 ,
PC_Memory_SPEC.Total_Paging_File_Space__0 ,
PC_Memory_SPEC.Total_Physical_Memory__KB0 from  MachineDataTable
,PC_Memory_COMM   , PC_Memory_SPEC where PC_Memory_COMM.datakey =*
CommonKey and PC_Memory_SPEC.datakey =* SpecificKey and ArchitectureKey = 5
and GroupKey = 9
GO
/****** Object:  View dbo.vProcessor    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vProcessor')
and sysstat & 0xf = 2)
```

```
drop view dbo.vProcessor
GO
Create View vProcessor as select dwMachineID ,
Processor_COMM.Processor_Name0 , Processor_COMM.Processor_Type0 ,
Processor_COMM.Quantity0 from  MachineDataTable  ,Processor_COMM   ,
Processor_SPEC where Processor_COMM.datakey =*  CommonKey and
Processor_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 6
GO
/****** Object:  View dbo.vServices    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vServices')
and sysstat & 0xf = 2)
drop view dbo.vServices
GO
Create View vServices as select dwMachineID , Services_SPEC.EXE_Path0 ,
Services_COMM.Name0 , Services_SPEC.Start_Name0 , Services_COMM.Start_Type0
, Services_COMM.State0 from  MachineDataTable  ,Services_COMM   ,
Services_SPEC where Services_COMM.datakey =*  CommonKey and
Services_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 13
GO
/****** Object:  View dbo.vVideo    Script Date: 7/5/95 4:30:47 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vVideo') and
sysstat & 0xf = 2)
drop view dbo.vVideo
GO
Create View vVideo as select dwMachineID , Video_COMM._nd_Adapter_Type0 ,
Video_COMM.Adapter_Type0 , Video_SPEC.Bios_Date0 ,
Video_COMM.Current_Video_Mode0 , Video_COMM.Display_Type0 ,
Video_COMM.Manufacturer0 , Video_COMM.Max_Rows0 from  MachineDataTable
,Video_COMM   , Video_SPEC where Video_COMM.datakey =*  CommonKey and
Video_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and GroupKey = 5
GO
/****** Object:  View dbo.vWorkstationStatus    Script Date: 7/5/95 4:30:47
AM ******/
if exists (select * from sysobjects where id =
object_id('dbo.vWorkstationStatus') and sysstat & 0xf = 2)
drop view dbo.vWorkstationStatus
GO
Create View vWorkstationStatus as select dwMachineID ,
WorkstationStatus.Failed_Hardware_Checks0 ,
WorkstationStatus.Files_Not_Installed0 , WorkstationStatus.LastHWScan ,
WorkstationStatus.LastSWScan , WorkstationStatus.Standalone_Workstation0 ,
WorkstationStatus.System_Files_Not_Modified0 from  MachineDataTable  ,
WorkstationStatus where WorkstationStatus.datakey =* SpecificKey and
```

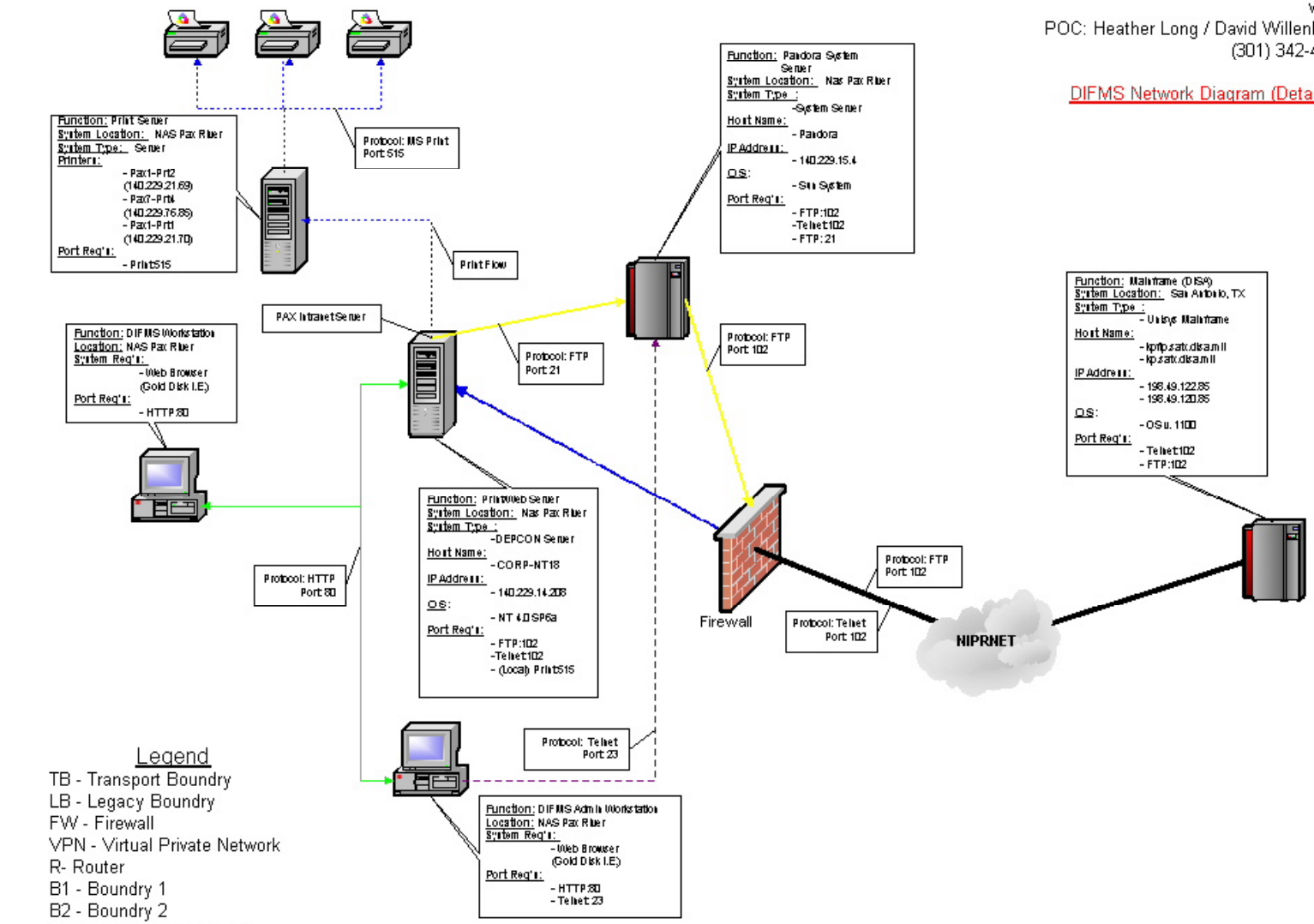
```
ArchitectureKey = 5 and GroupKey = 2
GO
```

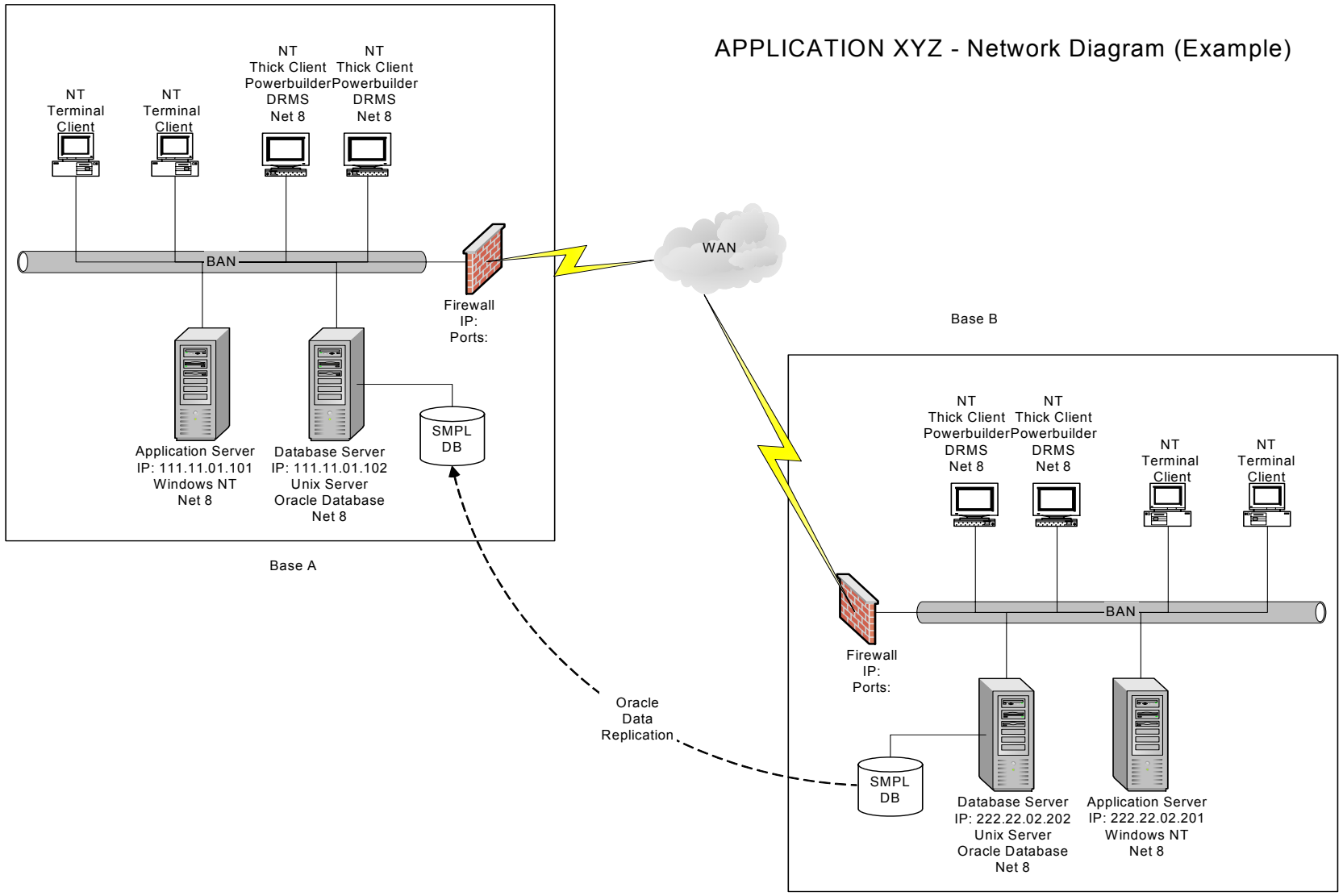
G5. Network Diagram Examples



RFS: 2274
Defense Industrial Financial Management System (DIFMS)
v.00A
POC: Heather Long / David Willenborg
(301) 342-4621

DIFMS Network Diagram (Detailed)




APPLICATION XYZ - Network Diagram (Example)
NT Terminal Client
NT Terminal Client
NT Thick Client Powerbuilder DRMS Net 8
NT Thick Client Powerbuilder DRMS Net 8
BAN
Firewall IP: Ports:
WAN
Application Server IP: 111.11.01.101 Windows NT Net 8
Database Server IP: 111.11.01.102 Unix Server Oracle Database Net 8
SMPL DB
Base A
Base B
NT Thick Client Powerbuilder DRMS Net 8
NT Thick Client Powerbuilder DRMS Net 8
NT Terminal Client
NT Terminal Client
BAN
Firewall IP: Ports:
Oracle Data Replication
SMPL DB
Database Server IP: 222.22.02.202 Unix Server Oracle Database Net 8
Application Server IP: 222.22.02.201 Windows NT Net 8

G6. Reachback and Datashare

Datashare/Reachback

Client		Datashare resources							Reachback						
User Name	Domain	Mapped Drives and Devices	Device or Service Name	Port	Protocol	IP Address	POC	Phone#	Desktop Name	IP	Router 1 IP	Router 2 IP	Router n... IP	Destination Name	IP
		1													
		2													
		3													
		4													
		Peripherals													
		Printers													
		Scanners													
		Other													
		Local Network Connections													
		Database													
		Server													
		Library													
		Peripheral													
		Other													
		Outer Network Connections													

Client		Datashare resources							Reachback						
User Name	Domain	Mapped Drives and Devices	Device or Service Name	Port	Protocol	IP Address	POC	Phone#	Desktop Name	IP	Router 1 IP	Router 2 IP	Router n... IP	Destination Name	IP
		1													
		2													
		3													
		4													
		Peripherals													
		Printers													
		Scanners													
		Other													
		Local Network Connections													
		Database													
		Server													
		Library													
		Peripheral													
		Other													
		Outer Network Connections													

G7. Legacy Server Template

Legacy Server Template

Site: _____
Date: _____
POC: _____
Address: _____
_____
PhoneNumber: _____
Email: _____

Line#	Serial Number	Name Server	Net Bios Name	IP Address	Gateway Address	Protocol	Domain Name	Fully Qualified Domin Name	Server Type	MAC Address	Operating System	Application Name	Version Number	Bus Type	Server Resources

Legacy Server Template Definitions

Line Number*	Sequential listing of assign assets (1,2,3...)
Serial Number*	The server's physical identification number
Name Server*	The unique name specifying a given path to the server's resources (ex. NCC.NCTS.NAVY.MIL)
NetBios Name*	Also called the computer name. The physical name of the server (ex. "finance", "cost analysis") note: 1) LMHost file contains mappings of IP Address to NetBios (computernames) i.e. 156.27.168.5 "Finance" 2) The Host file contains mappings of IP Addresses to Host Names i.e. 156.27.168.0 "finance. NAVY.MIL"
IP Address*	An identifier (name) for a computer or device on a TCP/IP network. The Servers logical address i.e. "172.68.156.5"
Gateway Address*	A node on a network that serves as an entrance to another network. The logical address of the intended network usually associated with a router i.e. "172. 16. 168.0"
Protocol*	Identify the internetworking protocol employed by the server
Domain Name*	A name which identifies one or more IP Address (navy.mil, ucla.edu, microsoft.com)
Fully Qualified Domain Name	(FQDN) A DNS domain name that has been stated unambiguously so as to indicate with absolute certainty its location in the domain namespace tree. Fully qualified domain names differ from relative names in that they are typically stated with a trailing period (.) - for example, host.example.microsoft.com. - to qualify their position to the root of the namespace. Locally, you can find the FQDN by running a trace route "tracert" on it's IP address.
Server Type*	Identify the generalfoverall function of the server
MAC Address*	Media Access Control Address: A hardware address which uniquely identifies a device on the network. The hardware address of a device connected to a shared network. Ex. It is the physical address of the server's NIC Card
Operating System*	The software platform on top of which all application programs run (i.e. Windows 95,98,NT,Unix)
Application Name*	List all application residing on the server
Version Number*	List the version number of each application
Bus Type*	List the bus specification for each application (i.e. 8,16,32 bit)
Server Resources	List all associated and miscellaneous applications residing on the server

* mandatory item

APPENDIX H – ENTERPRISE B1, B2, AND GPO AND OPERATIONAL MANAGEMENT

This appendix shows where B1 and B2 are implemented. Each boundary serves a purpose. The Boundary 1 (NOC) protects access to NIPRNet and Internet. The Boundary 2 performs similar functions as B1, except that the rules are more permissive for an interface with existing internal Navy and USMC networks.

Boundary Protection

Boundary Protections are the standard sets of protections that define the interfaces within NMCI and between NMCI and other networks. See Figure H-1 below. Boundary Protections enforce the policies required to connect to those external networks, provide security mechanisms for secure access to applications, and protect communities of interest (COIs) residing within NMCI. The type and strength of each security component is dependent upon the information protection requirements for a particular DON system. This is especially true for boundaries 1, 2 and 3. Boundary 1 reflects the Navy Marine Corps Enclave Protection Policy. Boundaries 2 and 3 security mechanisms are flexible enough to meet the security requirements of various scenarios. Specific configuration parameters of the security components deployed at the various boundary levels are tailored to provide the level of protection necessary to protect the confidentiality, integrity and availability, accountability and non-repudiation of NMCI.

GPO Overview

Group Policy is an Active Directory-based mechanism for controlling user and computer desktop environments in Windows 2000 domains. Settings for such items as security, software installation, and scripts can be specified through Group Policy. Group Policies are very simple to implement but can be quite complex to configure. Each GPO can consist of two parts: one that applies to a computer and one that applies to a user. GPOs can contain only computer policies, only user policies, or a mixture of the two. Group Policy is applied to groups of users and computers based on their location in the Active Directory. Group Policy allows the administrator to stipulate users' environments only once, and then rely on the operating system to enforce them thereafter.

Group Policy objects are not profiles. Profiles are user environment settings and are configurable by the user. Policies are standards configured by the administrator that are applied during computer boot-up and user log-on. They specify system behavior and restrict what users are allowed to do. Local policies are stored locally, within the computer's registry. Non-local policies are stored in the Active Directory. Local policies are not configured within the NMCI environment.

Group Policies are processed first at the site level, then the domain level, and finally at the organizational unit (OU) level. The administratively specified order determines the Group Policy settings that a user or computer actually receives. Furthermore, policy can be blocked at the Active Directory domain, or OU level.

Following are NMCI Group Policies:

- Account policies are applied at the NADSUSWE, NADSUSEA, MADSUS, and NMCI domains.
- User and computer policies are applied at the Command level OUs and below.
- Domain Controller policies are applied at the Domain Controller OU.
- Server policies are applied at the Application Services OU and below.
- Login script policies are applied where applicable.
- Workstation preference policies are applied at the Command level OUs.

Enterprise-wide permissions, parent to child domain (i.e., NADS to NADSUSWE) and domain to domain (i.e., NADSUSEA to NADSUSWE), and Group Policy propagation of permissions and traffic will exist but these practices will be scrutinized for performance issues.

Group Policy provides the following advantages:

- Integration with Windows 2000 Active Directory services
- Flexibility and scalability
- Provides an integrated tool for managing policy (MMC snap-in)
- Consistent and easy to use GPO snap-in
- Reliability and security

Operational Management

B1 Operational Management consists of the Office of the CNO (OPNAV N614) approving a common Enterprise Policy and ISF managing a policy-compliant operational configuration. To do this, ISF IA receives PIAB/LDSD&T trace data and recommends policy compliant Rulesets. ISF IA manages the Ruleset release, monitors implementation, and manages any legacy applications IA problems. ISF IA engineering develops policy-compliant firewall Rulesets. ISF IA then configures B1 firewall to include the released Rulesets. Finally, Wam!Net configures B1 router Access Control Lists (ACL) to duplicate firewall Rulesets. Figure I-3 shows the Boundary 1 Architecture.

B2 Operational Management consists of NETWARCOM approving a common Enterprise Policy and ISF managing a policy-compliant operational configuration. To do this, ISF IA develops policy-compliant Rulesets, receives PIAB/LDSD&T trace data and develops ACL mitigation rules. ISF IA manages the mitigation Ruleset release, monitors implementation, and manages any legacy applications IA problems. ISF IA also recommends common enterprise policy changes to NETWARCOM. ISF IA Transition configures B2 firewall to conform to the released common firewall Rulesets. Finally, Wam!Net configures B2 router ACLs to conform to released mitigation Ruleset. Figure I-4 shows the Boundary 2 Architecture.

GPO Operational Management involves NETWARCOM approving a common Enterprise Policy. This policy is known as WorkstationSEC (security). ISF IA reviews WorkstationSEC GPO rules and approves its release. ISF IA manages the policy-compliant operational configuration. ISF IA develops policy compliant GPO Rulesets, conducts vulnerability tests and issues Risk Assessment Reports. ISF IA also manages mitigation Ruleset release and recommends common enterprise policy changes to NETWARCOM. The NOC staff applies the Enterprise GPO to the Active Directory. GPO then replicates down to workstations throughout NMCI.

Figure H-1. Boundary Interfaces

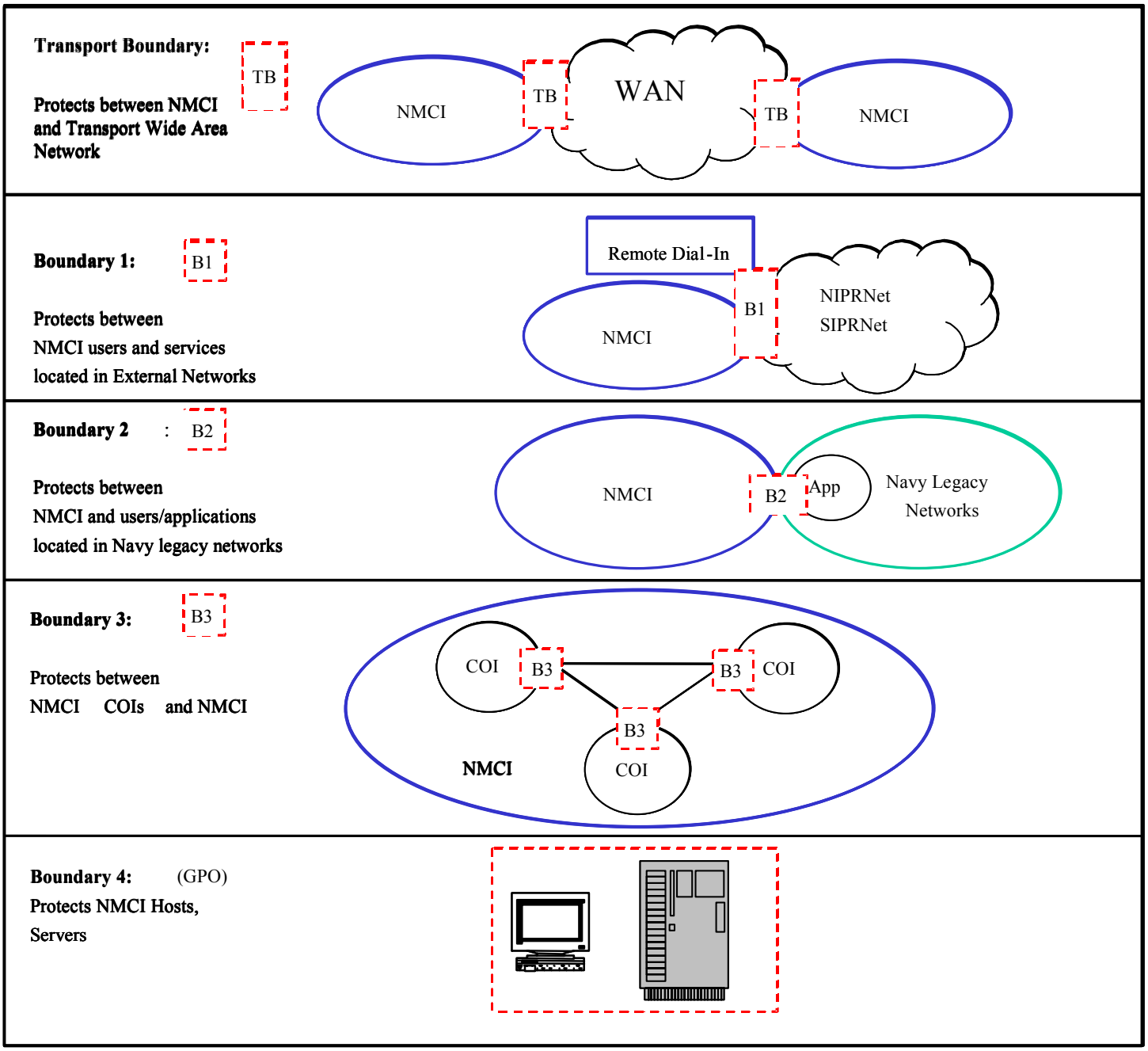


Figure H2. Simplified NMCI Architecture Overview

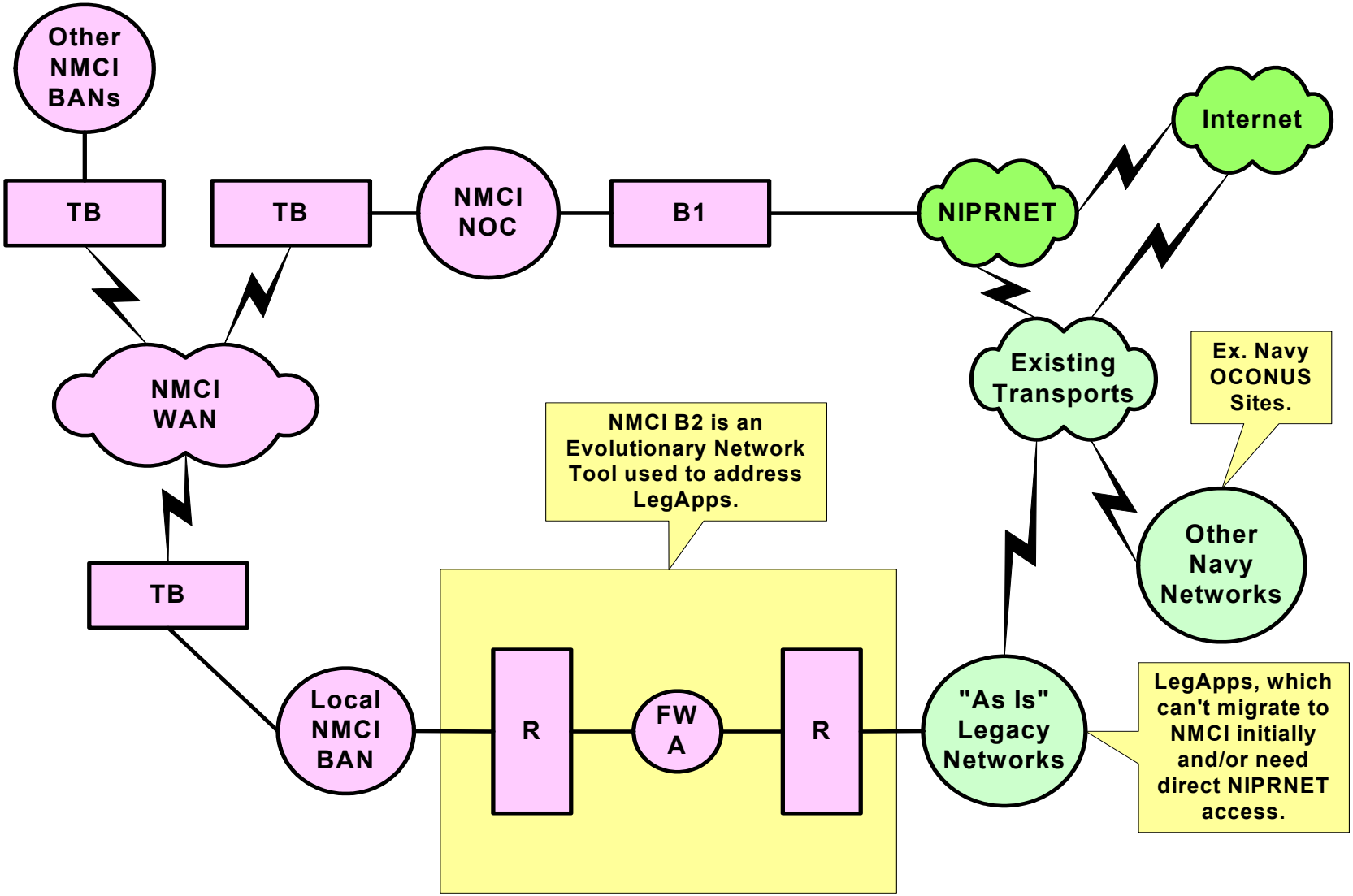


Figure H-3. Boundary 1 Architecture

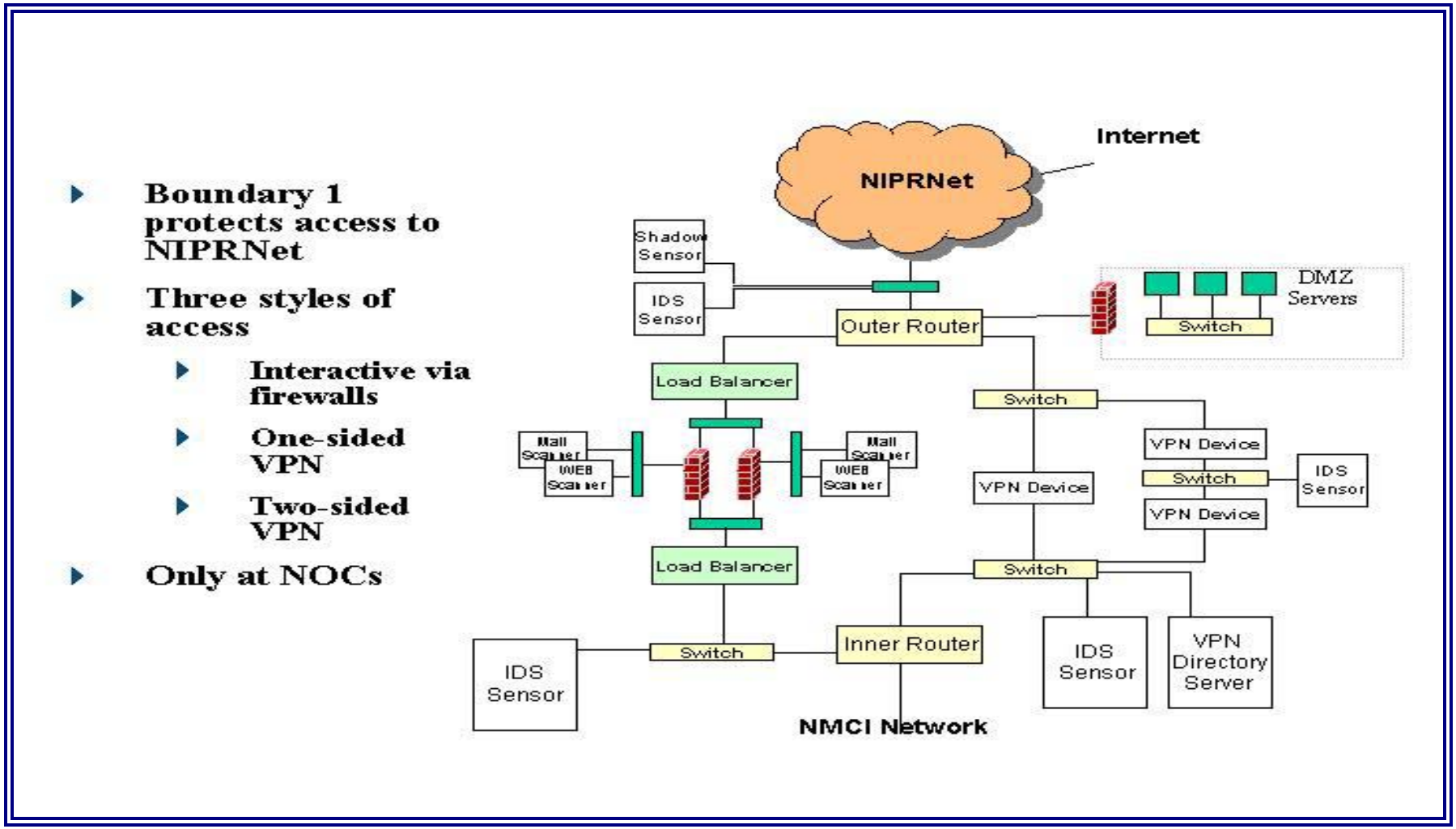
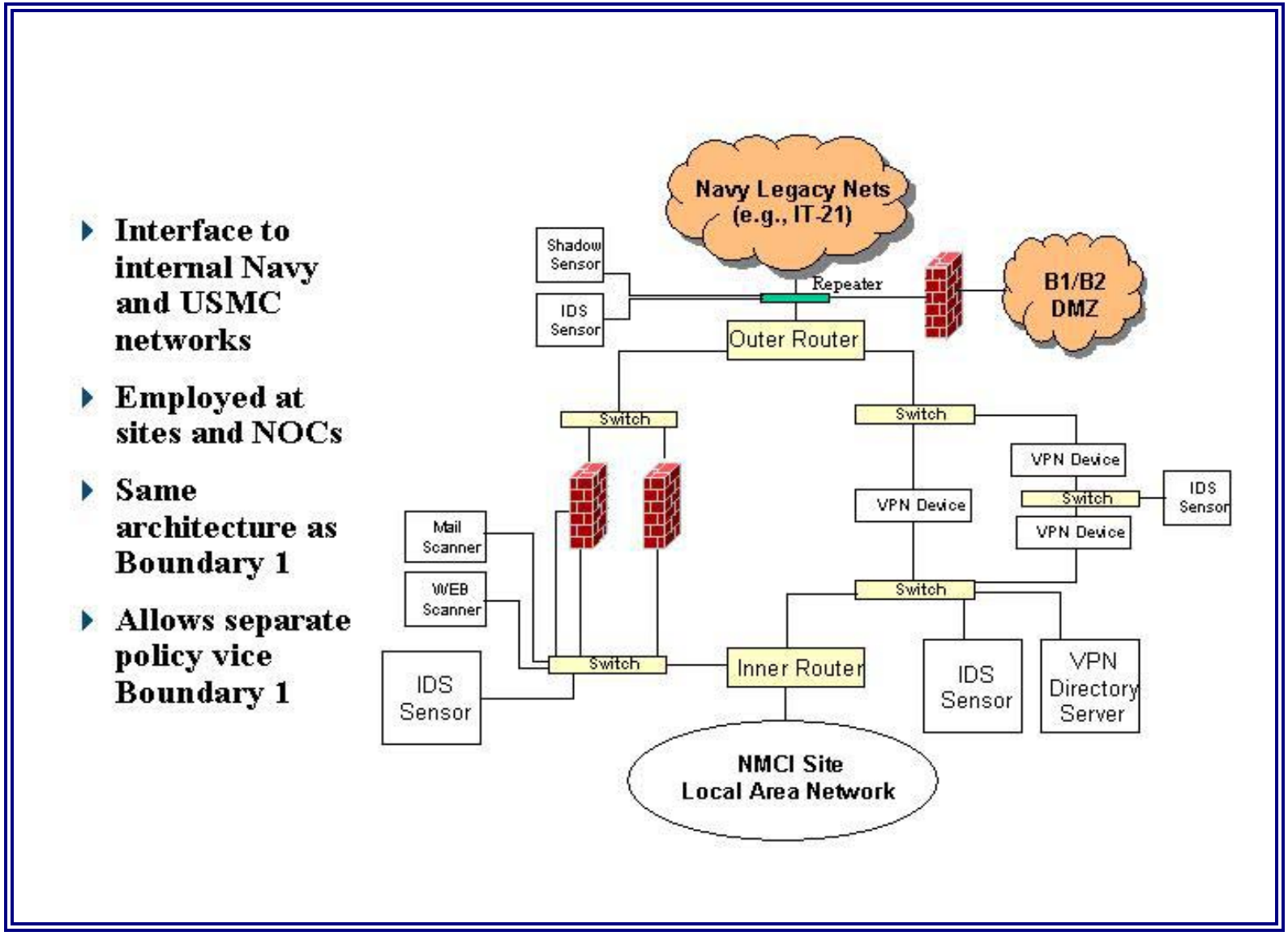


Figure H-4. Boundary 2 Architecture



APPENDIX I – GLOSSARY

Access: The availability of the full functionality of a system/application at the end-user desktop.

Accreditation: Formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. *Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary.*

Agent Software: Any software that monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.

Alpha Testing: A very early version of a software product that may not contain all of the features that are planned for the final version. Typically, software goes through two stages of testing before it is considered finished. Often, only users within the organization developing the software perform the first stage, called alpha testing. The second stage, called *beta testing*, generally involves a limited number of external users.

Application: (1) An automated software program that collects, stores, processes, and/or reports information in support of a specific user requirement. (2) Any software program that runs in a server-based or stand-alone environment that is used in a production capacity.

Application Development Software: Any software that generates or allows the user to create programming code which complies into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.

Application Mapping: The process of associating applications to users or to client machines is known as application mapping.

Application survey: The process of gathering COTS and GOTS application information necessary to rationalize or certify applications for migration to the NMCI environment. There are three categories of applications surveys: (1) desktop – a single user application not on the standard NMCI seat, (2) server-based, and (3) Web-based.

Assumption of Responsibility (AOR): The date when responsibility for operating the "as-is" environment and for work defined by the ordered NMCI CLINs shifts from the government and its local contractors to the Information Strike Force.

Beta Test: A test for a computer product prior to commercial release. Beta testing is the last stage of testing, and normally involves sending the product to *beta test sites* outside the company for real-world exposure. A round of testing called alpha testing often precedes beta testing.

Certification: The act of functionally testing an application for compatibility with the NMCI environment. This includes testing for Windows 2000 compatibility, Gold Disk interoperability, and GPO compliance, as well as compliance with Navy Boundary Policies. The NMCI Ruleset is enforced by the ISF at the time of certification testing.

Certification and Accreditation (C&A): The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the

accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. *Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary.* Includes testing the ability of the application to electronically distribute.

Client: The client part of *client-server architecture*. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an *e-mail client* is an application that enables you to send and receive e-mail.

Client-Server Architecture: A network architecture in which each computer or process on the network is either a *client* or a *server*. Servers are powerful computers or processes dedicated to managing disk drives (*file servers*), printers (*print servers*), or network traffic (*network servers)*. Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

Connectivity: The establishment and maintenance of a connection between two or more points in the NMCI. Categories of connectivity include:

Complex connectivity: Intranet connectivity involving systems/applications traversing protection boundaries internal to NMCI, but not Boundary 1, and extranet connectivity involving systems/ applications traversing NMCI boundaries, including Boundary 1, going external to NMCI.
Simple connectivity: Local area connections involving systems/applications that are active within a local area only and do not traverse internal or external NMCI boundaries.

Cutover: The actual event of rolling out NMCI desktops. Cutover follows the preparation phases pre-AOR and post-AOR of the legacy applications transition.

Cutover Start: In theory, Cutover begins at the pre-designated time when all pre-Cutover transition work is complete. Cutover actually begins upon the rollout of the first NMCI desktop at a site.
Cutover Complete: In theory, Cutover is complete when the final desktop and application is successfully deployed. In actuality, Cutover ends at the successful rollout of the last scheduled desktop.

Deployment: The delivery of an authorized application to a designated server or desktop through an automated or local deployment process.

Driver: Drivers are the associated software designed to allow peripherals to function with the workstation/desktop. They are defined as:

- Software that interfaces with a computer to a specific peripheral.
- A device driver is a program that controls a particular type of device that is attached to your computer. They are device drivers for printers, displays, CD-ROM readers, diskette drives, and so on. A device driver essentially converts the more general input/output instructions of the operating system to messages that the device type can understand.

Enterprise: Literally, a business organization. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. In this case, the entire NMCI environment.

Freeware: Copyrighted software given away for free by the author. Although it is available for free, the author retains the copyright, which means that one cannot do anything with it that is not expressly allowed by the author. Usually, the author allows people to use the software, but not sell it. Freeware is allowed in NMCI with approval of the FAM and NADTF.

Gameplan: The strategy devised before or used during an event. A strategy for reaching an objective. For NMCI, the Identification and Rationalization Gameplan is created to build the strategy a site will use to identify and rationalize their Legacy Applications.

Group Policy Object (GPO): a collection of settings that define what a system will look like and how it will behave for a defined group of users. GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs).

Kernel: The central module of an operating system. It is the part of the operating system that loads first, and it remains in main memory. Because it stays in memory, it is important for the kernel to be as small as possible while still providing all the essential services required by other parts of the operating system and applications. Typically, the kernel is responsible for memory management, process and task management, and disk management.

Legacy Application: An existing customer software application that is not included in the NMCI standard seat services or the CLIN 0023 catalog.

Local Deployment: The act of manually loading an authorized client application to the NMCI seat.

Mapping: To make logical connections between two entities. Within NMCI, mapping is primarily related to a connection to an Active Directory Object enabling access to applications, data, and peripherals. Mapping is also used within NMCI to associate users, applications, and peripherals to desktops/workstations.

Media: Objects on which data can be stored. These include hard disks, floppy disks, CD-ROMs, and tapes.

Metadata: Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses.

Migration: The process of moving from the use of one operating environment to another operating environment. For NMCI, this means moving from the existing network (legacy) to NMCI.

Mission-Critical System: A system handling information determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of content and timeliness. It must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). *Source: Navy IA Publication 5239-1*. Mission-critical systems are categorized as follows:

> Category 1: Defined by the Clinger/Cohen Act as National Security Systems (NSS) (intelligence activities; cryptologic activities related to national security; command and control of military forces, integral to a weapon or weapons system; systems critical to direct fulfillment of military or intelligence missions).

Category 2: In direct support of those systems identified by the Commanders in Chief (CINCs) which, if not functional, would preclude the CINC from conducting missions across the full spectrum of operations.
Category 3: Required to perform department-level and component-level core functions, including mission support.

NMCI Test Seat: An engineering tool used by ISF to test applications for compatibility with the NMCI environment. NMCI Test Seats are used when the NMCI infrastructure is in place and the end-to-end connectivity can be tested.

Peripheral: A computer device, such as a CD-ROM drive or printer, which is not part of the essential computer, i.e., the memory and microprocessor.

Point of Presence-In-A-Box (PoP-in-a-Box): An engineering tool used by ISF to test applications for compatibility with the NMCI environment. The PoP simulates the NMCI environment and consists of the Windows 2000 operating system, servers, and routers.

Push: The act of centrally managing and distributing authorized client software to the NMCI seat. In NMCI, this is accomplished through the use of Novadigm Radia. The Novadigm Radia Instance is loaded to the NMCI seat through an automated process called "push".

Quarantine: A Quarantined application is one that is not allowed to operate in the NMCI environment. Applications that are Quarantined are left to operate in the Legacy environment. Reasons for an application being Quarantined include: the application may not function in Win2K, it may interfere with the Gold Disk, it may violate GPO/B1/B2 policies, it may violate NMCI Ruleset, it may have been identified/submitted too late to process, it may have no user/tester support, or it may have a network connectivity error.

Rationalization: The process of identifying only those desktop and server-based applications, both COTS and GOTS, required to support Command or DON missions and goals. It includes the integration, consolidation, and elimination of applications and databases to improve standardization, enhance security, reduce duplication, and minimize support costs.

Repository: A secure place where information is stored for safekeeping.

Script: Another term for *macro* or batch file, a script is a list of commands that can be executed without user interaction. A *script language* is a simple programming language with which you can write scripts. For the Rapid Certification Phase, this refers to a "test script" used by the AIT lab to verify functionality of the application during testing.

Server: A computer or device on a network that manages network resources. For example, a *file server* is a computer and storage device dedicated to storing files.

Shareware: Software distributed on the basis of an honor system. Most shareware is delivered free of charge, but the author usually requests that one pay a small fee if one likes the program and uses it regularly. By sending the small fee, one becomes registered with the producer so that one can receive service assistance and updates. One can copy shareware and pass it along to friends and colleagues, but one must pay a fee if they use the product. According to the NMCI Ruleset, shareware is not authorized to operate in the NMCI environment.

System: (1) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *Source: Section 3502, Title 44, U.S. Code*.
(2) A group of interrelated and interdependent components, including applications, hardware, databases, and business procedures that, when combined, forms an organic whole and enables one or more functions.

SQL: Abbreviation of *structured query language*, and pronounced either *see-kwell* or as separate letters. SQL is a standardized query language for requesting information from a database.

URL: Abbreviation of *Uniform Resource Locator,* the global address of documents and other resources on the World Wide Web.

APPENDIX J – ACRONYM LIST

ACTR	Assistant Customer Technical Representative
ADS	Application Deployment Solution
AIS	Automated Information Systems
AIT	Application Integration and Testing
AOR	Assumption of Responsibility
ASNRDA	Assistant Secretary of the Navy for Research Development and Acquisition
ATO	Authority To Operate
B1	Boundary One
B2	Boundary Two
BLII	Base Level Information Infrastructure
CBA	Certification By Association
CCS	Claimant CDA Support
CDA	Central Design Authority/Central Design Activity/Central Development Activity
CIAT	Classified Application Integration and Testing
CIO	Chief Information Office
CJA	Critical Joint Applications
CLADRA	Classified Legacy Applications Deployment Readiness Activity
CLIN	Contract Line Item Number
CNNOC	Commander, Naval Network Operations Command
CNNWC	Command Navy Network Warfare Command
CNO	Chief of Naval Operations
CO	Commanding Officer
COR	Contract Officer's Representative
COTS	Commercial Off the Shelf
CPIAB	Classified PoP-In-A-Box
CPM	Customer Project Manager
CRFS	Classified Request For Service
CTR	Customer Technical Representative
DAA	Designated Approval Authority
DADMS	DON Application and Database Management System
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMT	Data Management Team
DNS	Domain Name System
DoD	Department of Defense
DON	Department of the Navy
DSL	Definitive Software Library
EAGLE	Enterprise Application Group for Legacy and Emerging
EDS	Electronic Data Systems
EDSL	Enterprise Definitive Software Library
EQRC	Enterprise Quarantine Reduction Coordinator
ERQ	Engineering Review Questionnaires
ESO	Enterprise Solution Office

FAM	Functional Area Manager
FDA	Functional Data Administrator
FOUO	For Official Use Only
FTP	File Transfer Protocol
GOTS	Government Off the Shelf
GPO	Group Policy Object
HVAC	Heating, Ventilation, Air Conditioning
IA	Information Assurance
IATO	Interim Authority To Operate
IATC	Interim Authority to Connect
IATT	Information Assurance Tiger Team
IRAAD	Issues, Risks, Actions, Assumptions, Decisions
IQRPL	IATT Quarantine Remediation Priority List
ISF	Information Strike Force
ISFTDB	ISF Tools Database
IT/IM	Information Technology/Information Management
IT-21	Information Technology for the 21st Century
JECCC	Joint Enterprise Command & Control Center
LADRA	Legacy Application Deployment Readiness Activity
LAPOC	Legacy Application Point of Contact
LAQRG	Legacy Application Quarantine Remediation Guide
LATF	Legacy Application Task Force
LATG	Legacy Applications Transition Guide
LDSD&T	Local Deployment Solution Development and Testing
MCTN	Marine Corps Tactical Network
MSI	Microsoft Installer
NADTF	Navy Applications Database Task Force
NAT	Network Address Translation
Navy IO	Navy Information Officer
NCARP	NMCI Connection Approval Review Panel
NEADG	Navy Enterprise Application Development Guide
NET	NMCI Enterprise Tool
NETWARCOM	Naval Network Warfare Command
NMCEPP	Navy Marine Corps Enclave Protection Policy
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NOIS	NMCI Ordering Interface System
OCONUS	Outside Continental United States

PCL	Proving Center Lab
PDA	Product Delivery Analyst, Personal Digital Assistant
PDM	Product Delivery Manager
PEO-IT	Program Executive Office for Information Technology
PIAB	Pop-In-A-Box
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Program of Record
PSI	Physical Site Identifier
POR	Program of Record
QRG	Quarantine Remediation Group
QRP	Quarantine Reduction Process
RFS	Request for Service
RMERQ	Risk Mitigation Engineering Review Questionnaire
S&T	Science and Technology
SIL	Site Integration Lead
SM	Site Manager
SME	Subject Matter Expert
SPAWAR	Space and Naval Warfare Systems Command
SSAA	Systems Security Authorization Agreement
SSE	Site Solutions Engineering
STEM	Site Transition Execution Manager
TFWeb	Task Force Web
URL	Uniform Resource Locator
VPN	Virtual Private Network
WIT	Waiver Input Template